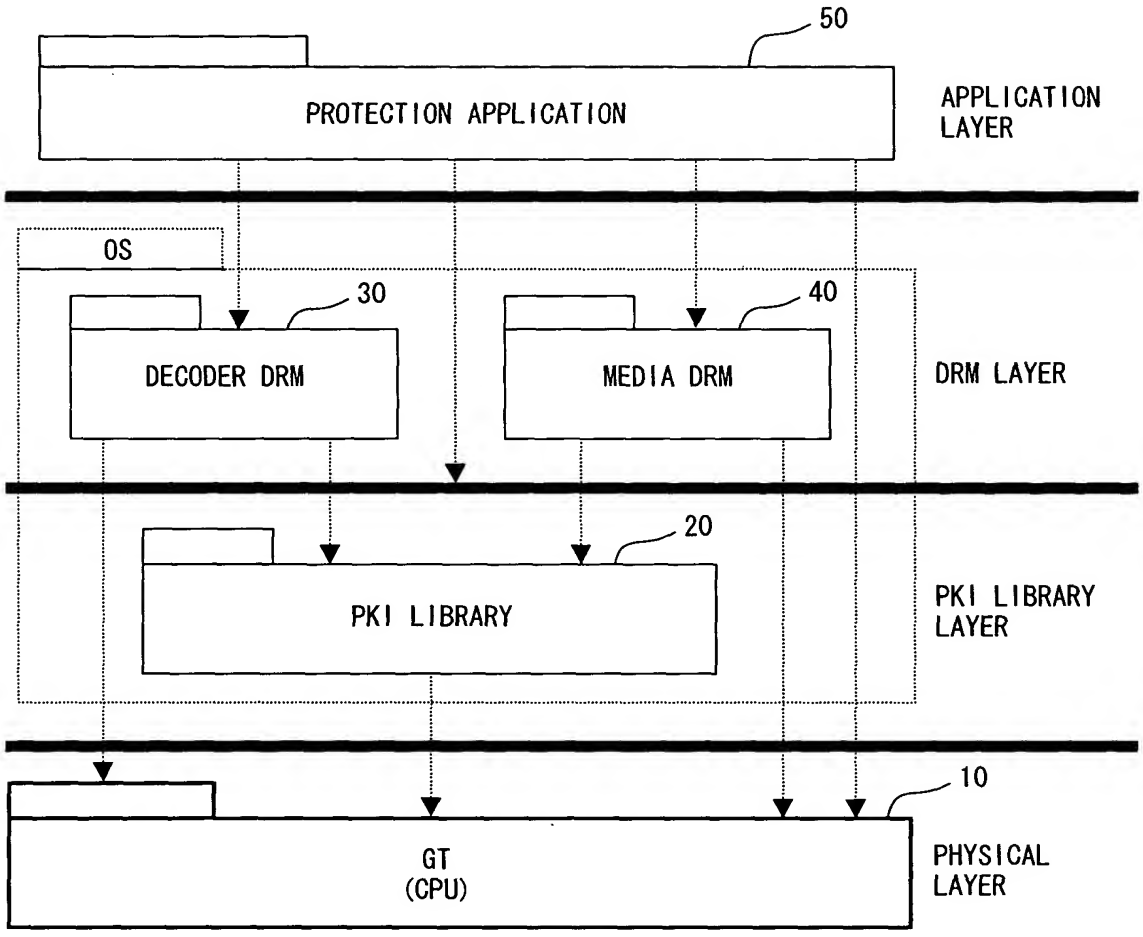

50
PROTECTION APPLICATION
APPLICATION LAYER
OS
30
40
DECODER DRM
MEDIA DRM
DRM LAYER
20
PKI LIBRARY
PKI LIBRARY LAYER
10
GT
(CPU)
PHYSICAL LAYER

FIG. 1

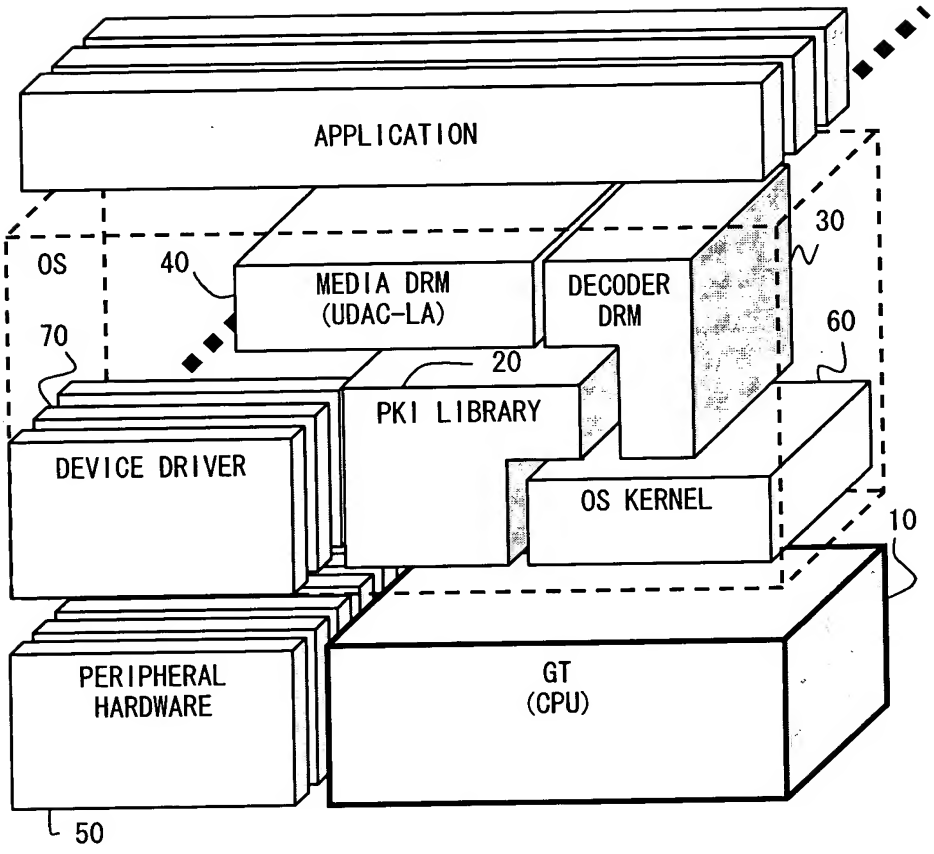

APPLICATION
OS
40
MEDIA DRM
(UDAC-LA)
DECODER
DRM
30
60
70
20
PKI LIBRARY
DEVICE DRIVER
OS KERNEL
10
PERIPHERAL
HARDWARE
GT
(CPU)
50

FIG. 2

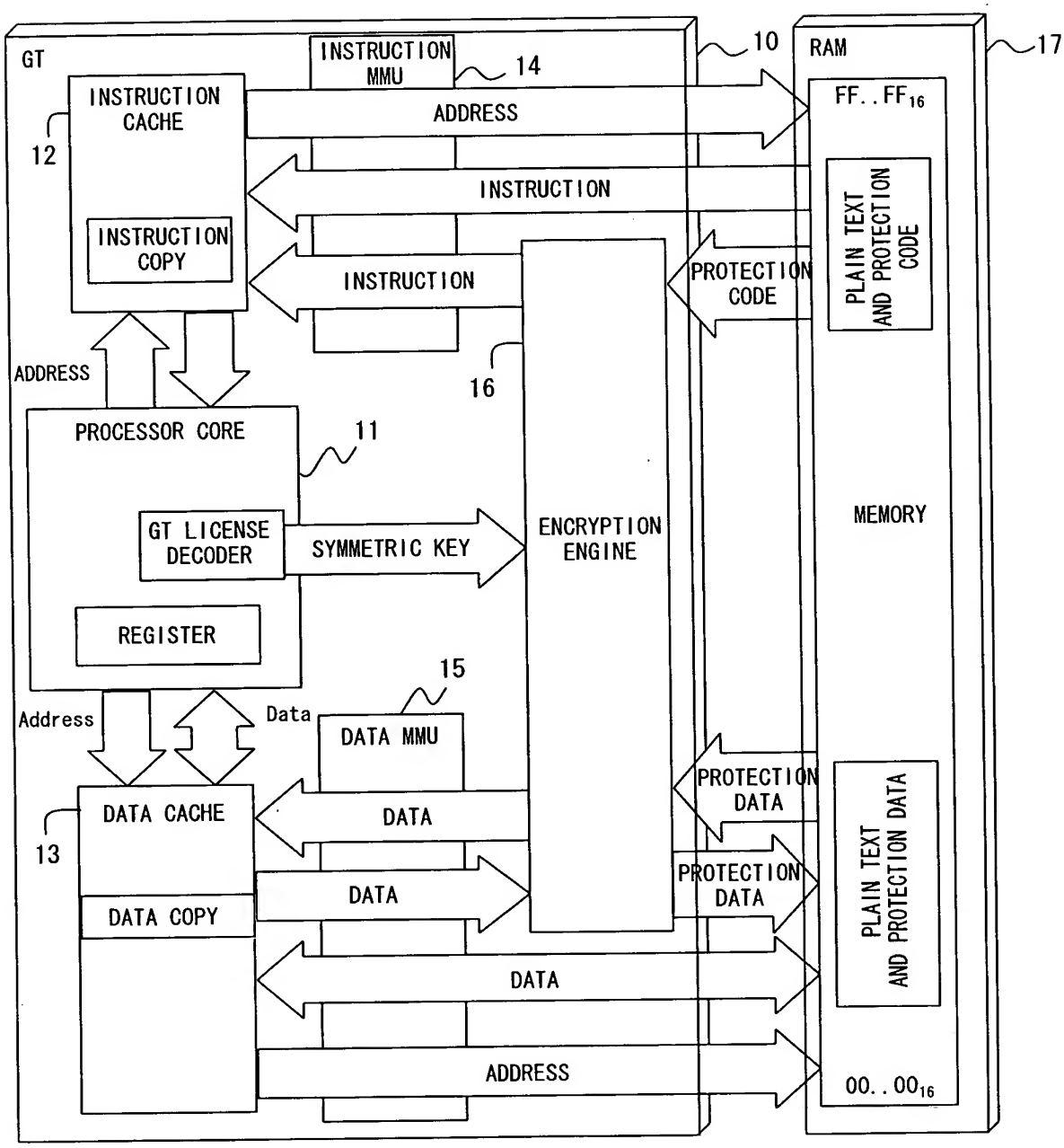

GT
INSTRUCTION MMU
14
10
RAM
17
INSTRUCTION CACHE
12
ADDRESS
FF..FF16
INSTRUCTION
INSTRUCTION COPY
INSTRUCTION
PROTECTION CODE
PLAIN TEXT AND PROTECTION CODE
ADDRESS
16
PROCESSOR CORE
11
GT LICENSE DECODER
SYMMETRIC KEY
ENCRYPTION ENGINE
MEMORY
REGISTER
15
Address
Data
DATA MMU
PROTECTION DATA
DATA CACHE
13
DATA
DATA
PROTECTION DATA
PLAIN TEXT AND PROTECTION DATA
DATA COPY
DATA
ADDRESS
00..00₁₆

FIG. 3

Notation	Field Size	Name	Description
p	1 bit	Present flag	IF ON (1), THIS INDICATES THAT TRB IS VALID.
uo	1 bit	Unable to Output	IF ON (1), THIS INDICATES THAT CONTENT IS NOT OUTPUT.
cl	1 bit	Cache Lock	IF ON (1), THIS INDICATES THAT DATA ON TAMPER RESISTANT PAGE SPECIFIED WITH kid IS NOT OUTPUT TO OUTSIDE OF CACHE.
kid	20 bits OR SO	Key ID	INFORMATION FOR LINK FROM TLB.
key	128 bits OR MORE	Cryptographic Key	VALUE OF ENCRYPTION/DECRYPTION KEY OF CODE OR DATA ON PAGE LINKED TO THIS LINE. KEY OF SYMMETRIC (COMMON) KEY CRYPTOSYSTEM.
ackey	SAME AS key	Authorized code key	DECRYPTION KEY (key OF ANOTHER OR OWN LINE) OF EXECUTABLE CODE OF PROTECTION PROCESS PERMITTED TO ACCESS PAGES OF ALL TLB LINES INCLUDING kid.
eadr	64 bits OR SO	Exception address	START ADDRESS OF EXCEPTION PROCESS CODE WHICH OCCURS IMMEDIATELY BEFORE RESTORATION IS MADE FROM PAGE HAVING DIFFERENT key TO PAGE LINKED TO THIS TRB LINE.

FIG. 4

Notation		Field Size	Name	Description
p		1 bit	Present flag	INDICATES THAT TLB IS VALID
id		20 bit OR SO	Region Identifier	IDENTIFIER VALUE OF PAGE REGION INDICATED BY CORRESPONDING LINE WITHIN TLB
ppn		32 bits OR SO	Physical page number	PHYSICAL PAGE NUMBER OF CONVENTIONAL TLB.
vpn		56 bits OR SO	Virtual page number	VIRTUAL PAGE NUMBER OF CONVERSIONAL TLB.
rights	pl	2 bit	Privilege level	PRIVILEGE LEVEL ACCESSIBLE TO PAGE. FOR DETAILS, SEE FIGS. 6 AND 7.
	ar	3 bit	Access Rights	PRIVILEGE LEVEL ACCESSIBLE TO PAGE. FOR DETAILS, SEE FIGS. 6 AND 7.
	tr	1 bit	Tamper Resistance	IF ON (1), THIS INDICATES THAT PAGE EXISTS IN TAMPER RESISTANT SEGMENT SPACE, AND CORRESPONDING LINE EXISTS IN TRB.
	df	1 bit	Debug mode Flag	VALID ONLY IF tr IS ON (1). IF tr AND df ARE ON, DEBUG MORE SPECIFIED ACCORDING TO ar RUNS.
kid		20 bits OR SO	Key ID	IDENTIFICATION INFORMATION OF TRB LINE (INSERTION) FOR LINKING TO KEY INFORMATION WITHIN TRB.
ebim		3 bits OR SO	Encrypted Block Identification	COPIED VALUE OF ACgt.ebim OF GT LICENSE. THIS VALUE BECOMES 0 IF tr IS OFF.
sign		128 bits OR SO	Digital signature	DIGITAL SIGNATURE VALUE OBTAINED BY CONCATENATING FIELDS FROM vpn TO ebim. GENERATED BY GT.

FIG. 5

PRS. S EXECUTION MODE	PTE. TR (TLB. tr)	PTE. PP (TLB. ar)	IF (INSTRUCTION FETCH)	Load (LOAD INSTRUCTION	Store (STORE INSTRUCTION
1 SUPERVISOR MODE	0 NORMAL	000	OK	OK	OK
		001	OK	OK	NG
		010	OK	NG	NG
		011	NG	NG	NG
	1 TAMPER RESISTANT	000	SPECIFIED MODE	SPECIFIED MODE	SPECIFIED MODE
		001	SPECIFIED MODE	SPECIFIED MODE	NG
		010	SPECIFIED MODE	NG	NG
		011	NG	NG	NG
0 USER MODE	0 NORMAL	100	OK	OK	OK
		101	OK	OK	NG
		110	OK	NG	NG
		111	NG	NG	NG
	1 TAMPER RESISTANT	100	SPECIFIED MODE	SPECIFIED MODE	SPECIFIED MODE
		101	SPECIFIED MODE	SPECIFIED MODE	NG
		110	SPECIFIED MODE	NG	NG
		111	NG	NG	NG

FIG. 6

TLB.rights		TLB.pl	Process Privilege Level				Description
tr&df	ar		3	2	1	0	
tr=0	0	3	R	R	R	R	ONLY read
		2	–	R	R	R	
or		1	–	–	R	R	
		0	–	–	–	R	
	1	3	RX	RX	RX	RX	read, execute
tr=1,		2	–	RX	RX	RX	
		1	–	–	RX	RX	
		0	–	–	–	RX	
	2	3	RW	RW	RW	RW	read, write
		2	–	RW	RW	RW	
		1	–	–	RW	RW	
		0	–	–	–	RW	
	3	3	RWX	RWX	RWX	RWX	read, write, execute
		2	–	RWX	RWX	RWX	
		1	–	–	RWX	RWX	
		0	–	–	–	RWX	
tr=1,	0	3	PR	PR	PR	PR	ONLY read FROM SPECIFIED
df=0		2	–	PR	PR	PR	PROCESS
		1	–	–	PR	PR	
		0	–	–	–	PR	
	1	3	X	X	X	X	execute AND read FROM
		2	–	X	X	X	SPECIFIED PROCESS
		1	–	–	X	X	
		0	–	–	–	X	
	2	3	PRW	PRW	PRW	PRW	read AND write FROM
		2	–	PRW	PRW	PRW	SPECIFIED PROCESS
		1	–	–	PRW	PRW	
		0	–	–	–	PRW	
	3	3	PWX	PWX	PWX	PWX	read, write, AND execute
		2	–	PWX	PWX	PWX	FROM SPECIFIED PROCESS
		1	–	–	PWX	PWX	
		0	–	–	–	PWX	

FIG. 7

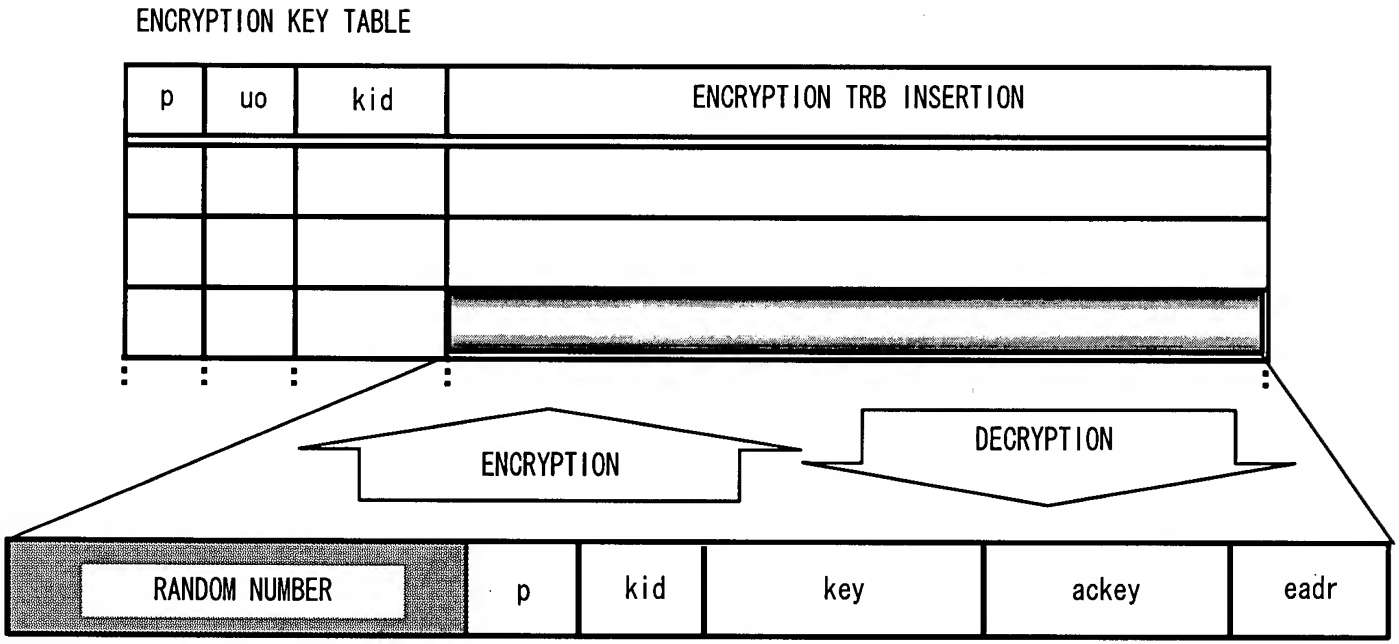

ENCRYPTION KEY TABLE
p
uo
kid
ENCRYPTION TRB INSERTION
ENCRYPTION
DECRYPTION
RANDOM NUMBER
p
kid
key
ackey
eadr

FIG. 8

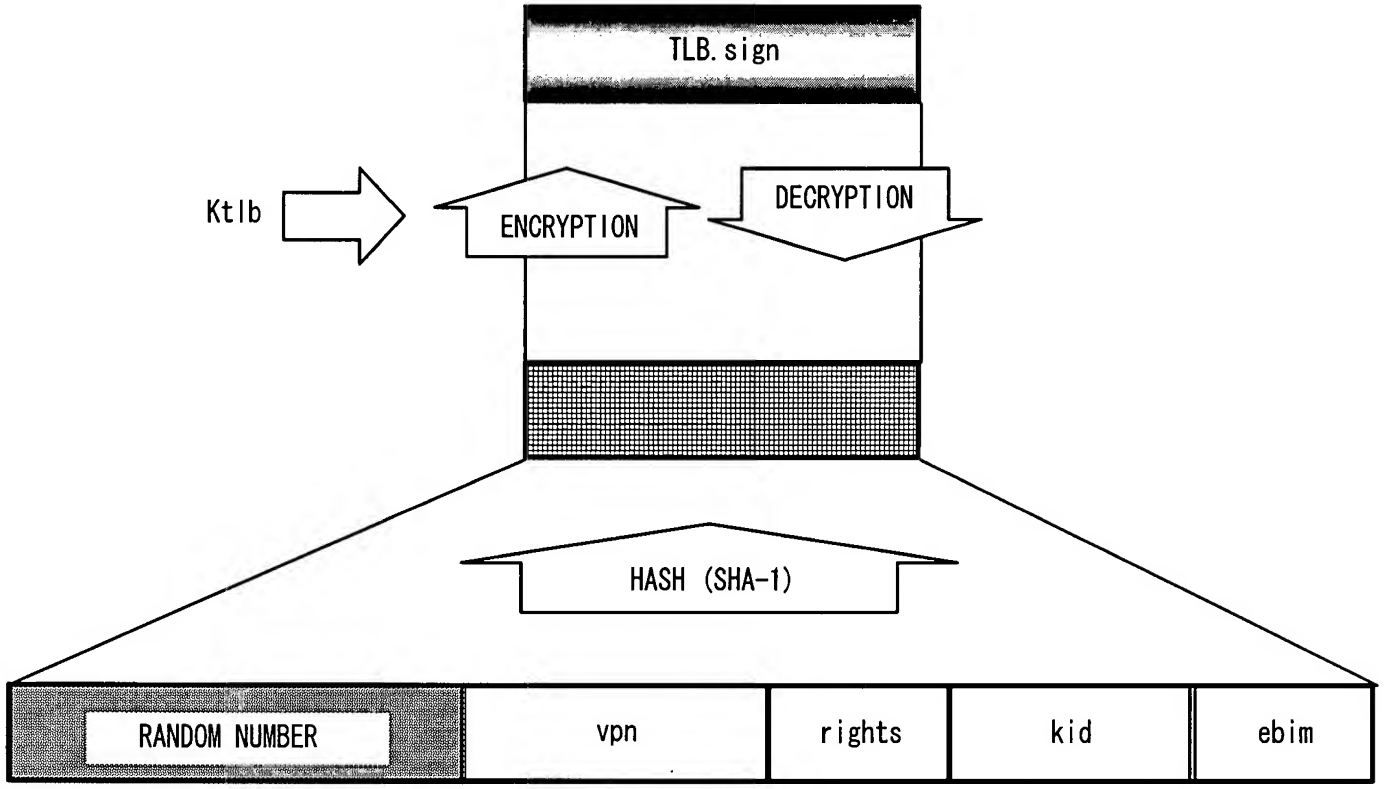

TLB.sign
Ktlb
ENCRYPTION
DECRYPTION
HASH (SHA-1)
RANDOM NUMBER
vpn
rights
kid
ebim

FIG. 9

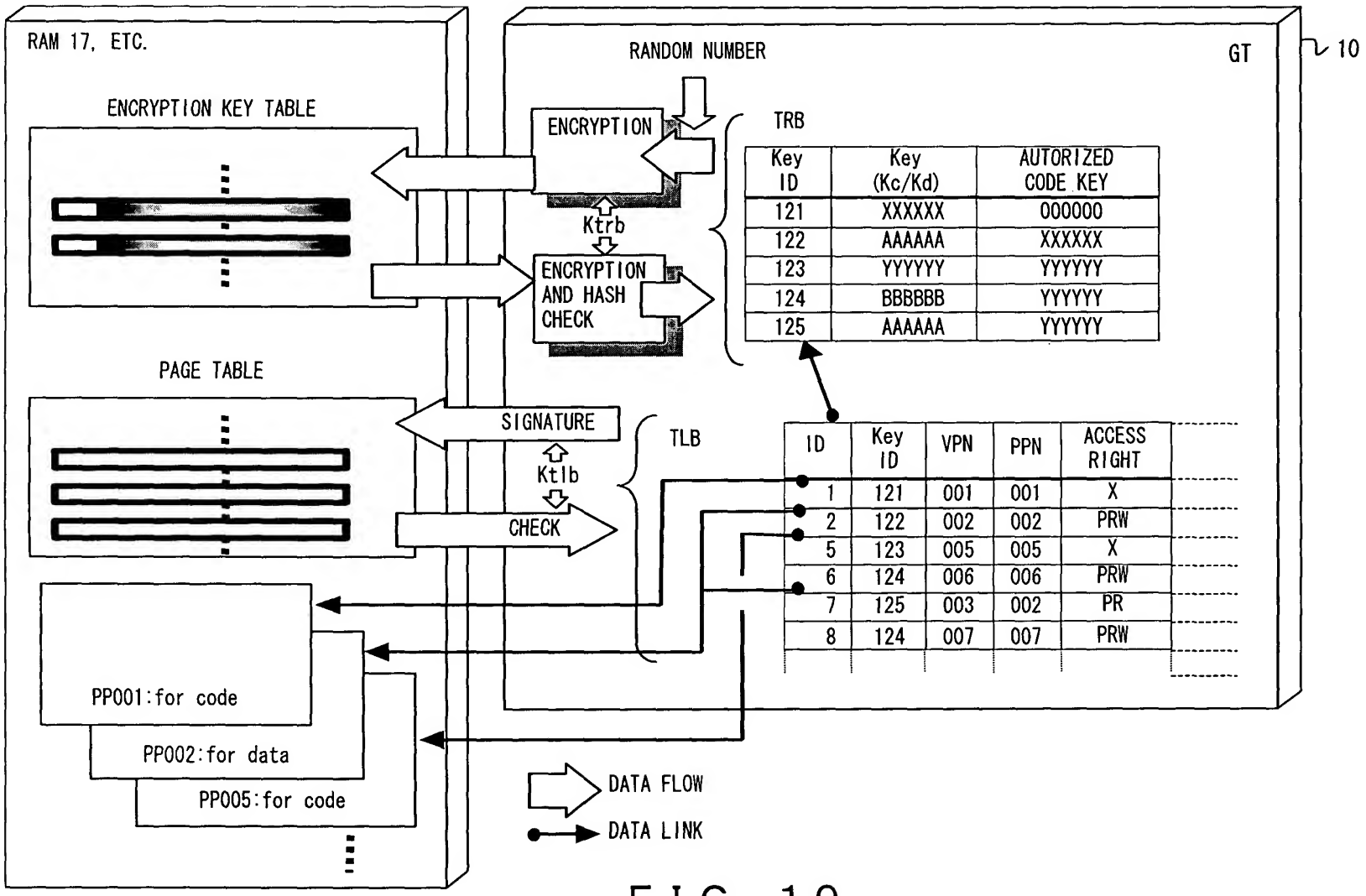

RAM 17, ETC.
RANDOM NUMBER
GT
10
ENCRYPTION KEY TABLE
ENCRYPTION
Ktrb
ENCRYPTION AND HASH CHECK
TRB
Key ID
Key (Kc/Kd)
AUTORIZED CODE KEY
121 XXXXXX 000000
122 AAAAAA XXXXXX
123 YYYYYY YYYYYY
124 BBBBBB YYYYYY
125 AAAAAA YYYYYY
PAGE TABLE
SIGNATURE
Ktlb
CHECK
TLB
ID
Key ID
VPN
PPN
ACCESS RIGHT
1 121 001 001 X
2 122 002 002 PRW
5 123 005 005 X
6 124 006 006 PRW
7 125 003 002 PR
8 124 007 007 PRW
PP001:for code
PP002:for data
PP005:for code
DATA FLOW
DATA LINK

FIG. 10

Notation	Field Size	Name	Description
trss	1 bit	Tamper Resistant Segment Selector	IF ON, TAMPER RESISTANT SPACE IS SELECTED, IF OFF, NORMAL VIRTUAL SPACE IS SELECTED.

FIG. 11

Notation	Field Size	Name	Description
rid	8 bits OR SO	Register ID	ID SPECIFYING REGISTER.
seal	1 bit	Seal flag	IF ON (1), THIS INDICATES THAT REGISTER IS BEING SEALED. IF OFF (0), THIS INDICATES THAT REGISTER IS RELEASED.
ackey	SAME AS TRB.key	Authorized code key	Key TO CODE PAGE OF PROCESS PERMITTED TO ACCESS REGISTER.

FIG. 12

Notation	Field Size	Name	Description
r1ss	1 bit	Resister 1 Seal Status	IF ON (1), THIS INDICATES THAT r1 IS BEING SEALED. IF OFF (0), THIS INDICATES THAT r1 IS RELEASED.
r2ss	1 bit	Register 2 Seal Status	IF ON (1), THIS INDICATES THAT r2 IS BEING SEALED. IF OFF (0), r2 IS RELEASED.

FIG. 13

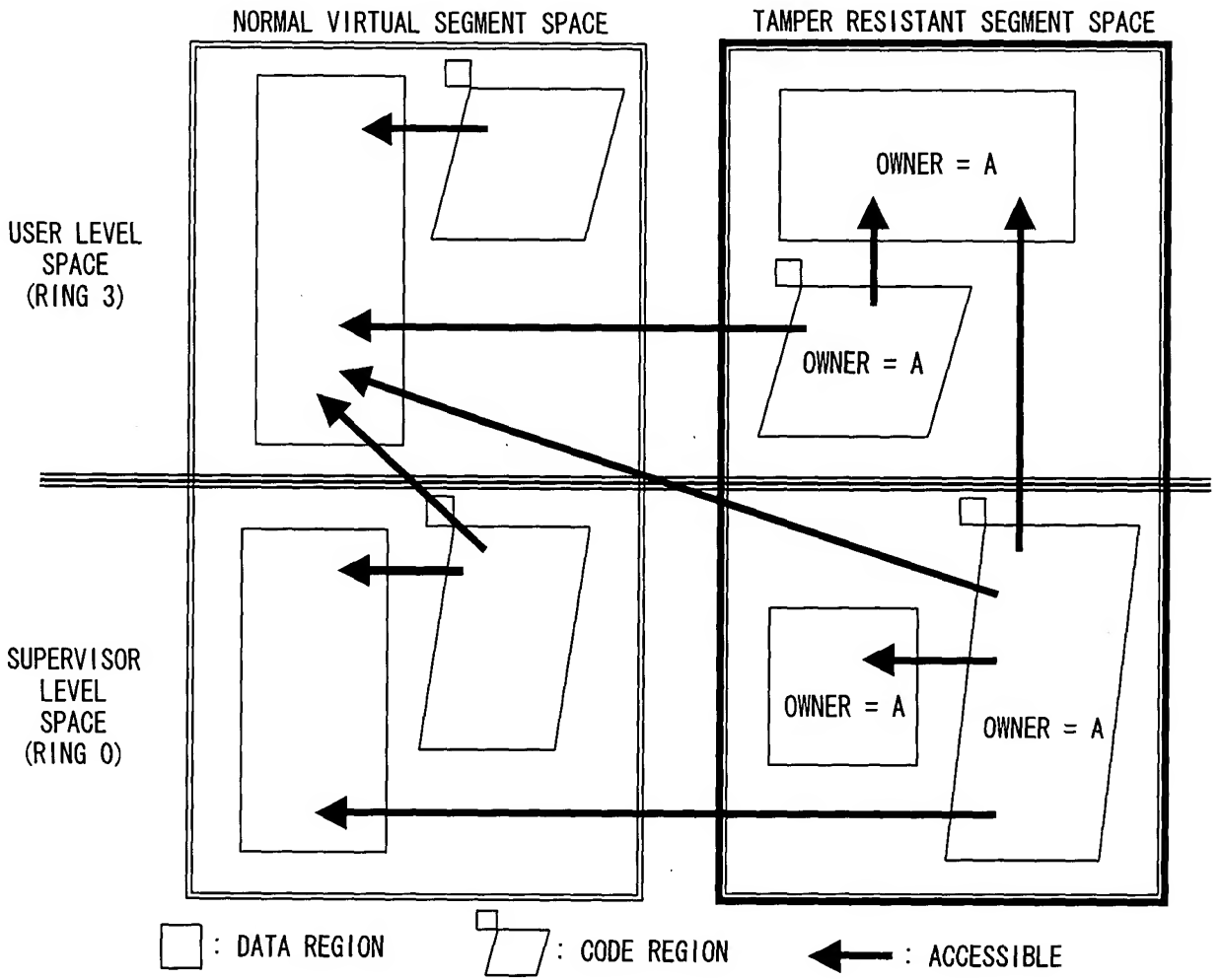

NORMAL VIRTUAL SEGMENT SPACE
TAMPER RESISTANT SEGMENT SPACE
USER LEVEL SPACE (RING 3)
SUPERVISOR LEVEL SPACE (RING 0)
OWNER = A
OWNER = A
OWNER = A
OWNER = A
: DATA REGION
: CODE REGION
: ACCESSIBLE

FIG. 14

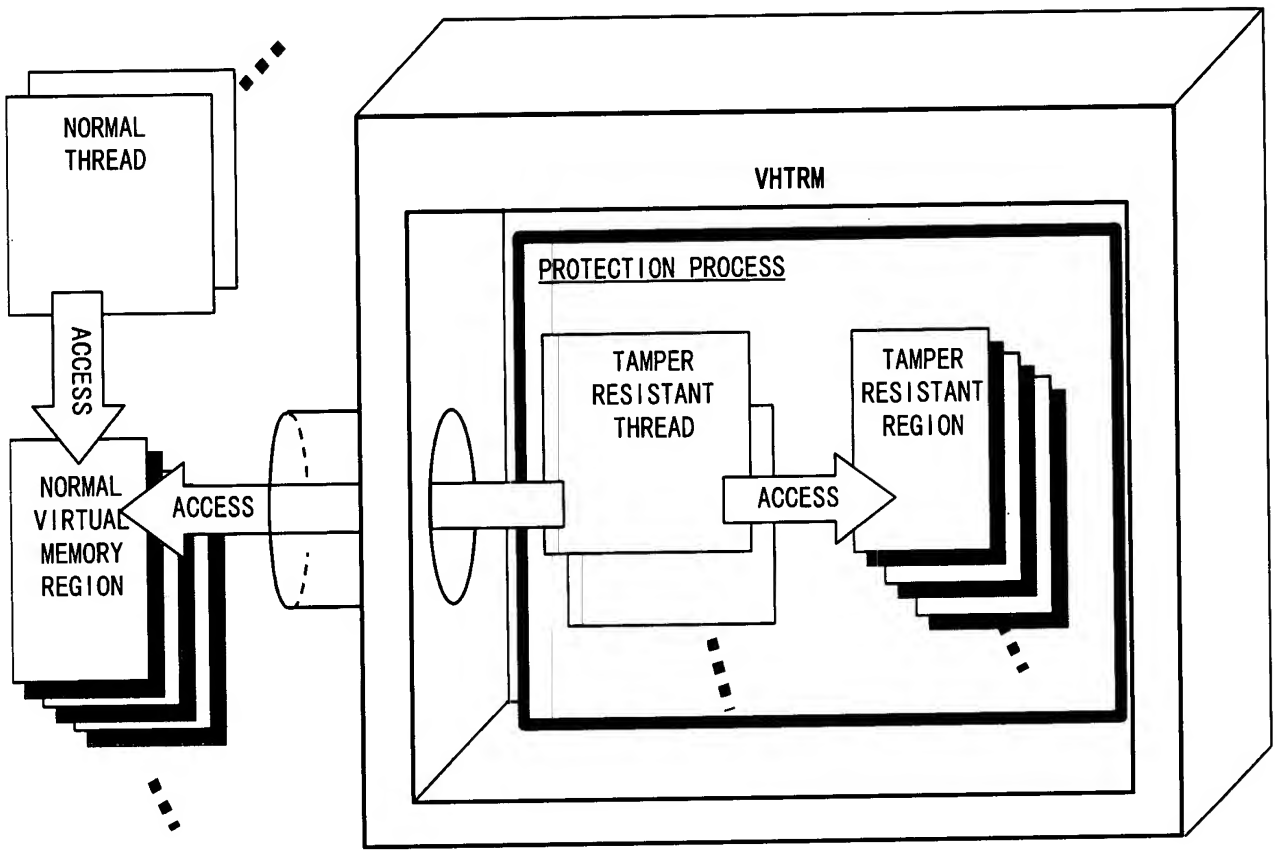

NORMAL THREAD
ACCESS
NORMAL VIRTUAL MEMORY REGION
ACCESS
VHTRM
PROTECTION PROCESS
TAMPER RESISTANT THREAD
ACCESS
TAMPER RESISTANT REGION

FIG. 15

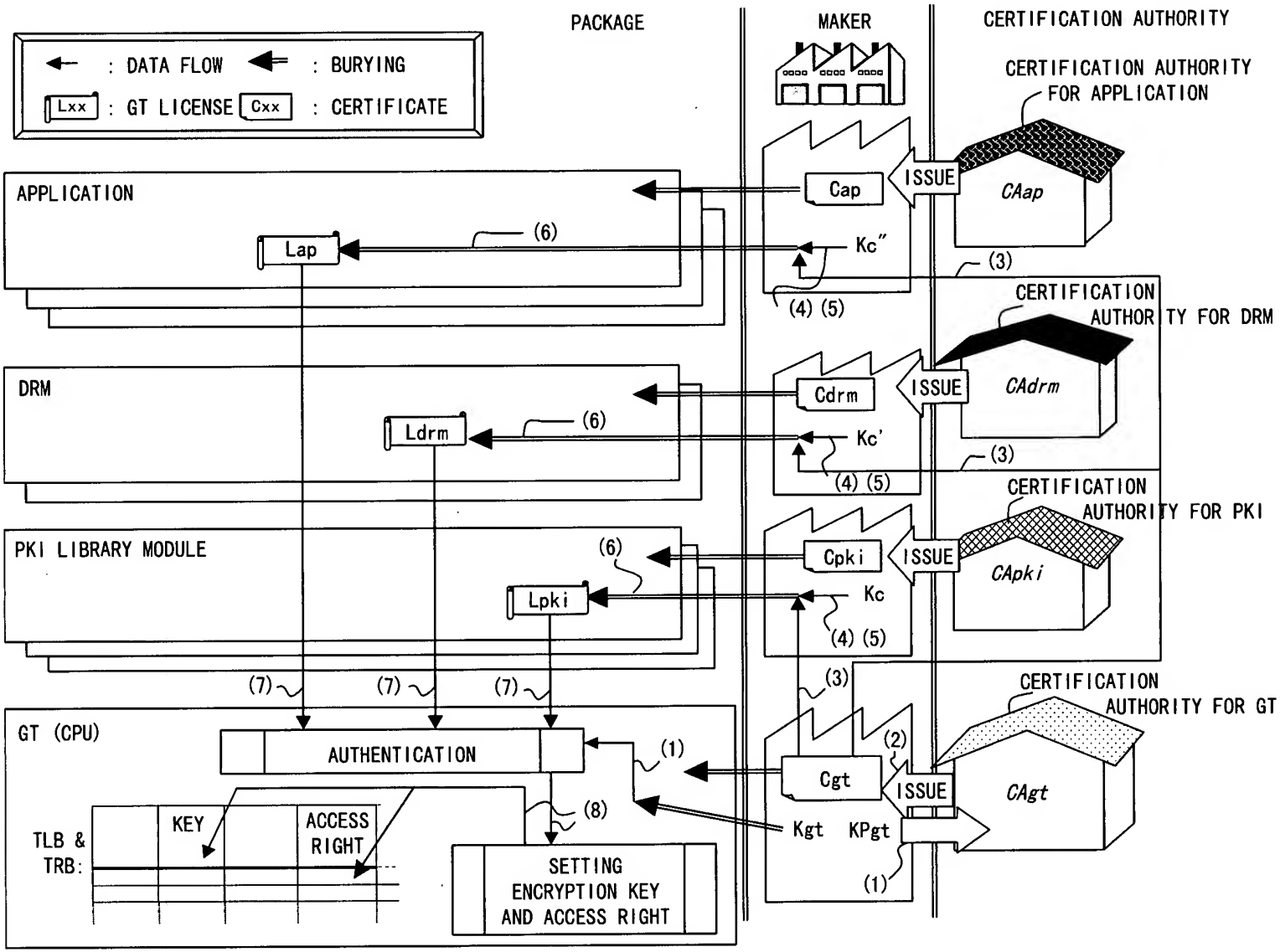

: DATA FLOW
: BURYING
Lxx : GT LICENSE
Cxx : CERTIFICATE
PACKAGE
MAKER
CERTIFICATION AUTHORITY
CERTIFICATION AUTHORITY FOR APPLICATION
APPLICATION
Lap
(6)
Cap
ISSUE
CAap
Kc"
(3)
(4) (5)
CERTIFICATION AUTHORITY FOR DRM
DRM
Ldrm
(6)
Cdrm
ISSUE
CAdrm
Kc'
(3)
(4) (5)
CERTIFICATION AUTHORITY FOR PKI
PKI LIBRARY MODULE
(6)
Lpki
Cpki
ISSUE
CApki
Kc
(4) (5)
(7)
(7)
(7)
(3)
CERTIFICATION AUTHORITY FOR GT
GT (CPU)
AUTHENTICATION
(1)
(2)
Cgt
ISSUE
CAgt
(8)
TLB & TRB:
KEY
ACCESS RIGHT
Kgt
KPgt
(1)
SETTING ENCRYPTION KEY AND ACCESS RIGHT

FIG. 16

SYMBOL	DECRYPTION	read RIGHT	write RIGHT	execute RIGHT
PR	READ CAN BE MADE ONLY FROM SPECIFICATION CODE	SPECIFICATION CODE*1	NONE	NONE
X (PRX)	READ AND EXECUTION CAN BE MADE FROM SPECIFICATION CODE	SPECIFICATION CODE*1	NONE	SPECIFICATION CODE*1
PRW	READ AND WRITE CAN BE MADE FROM SPECIFICATION CODE	SPECIFICATION CODE*1	SPECIFICATION CODE*1	NONE
PWX (PRWX)	READ AND WRITE CAN BE MADE FROM SPECIFICATION CODE	SPECIFICATION CODE*1	SPECIFICATION CODE*1	SPECIFICATION CODE*1

FIG. 17

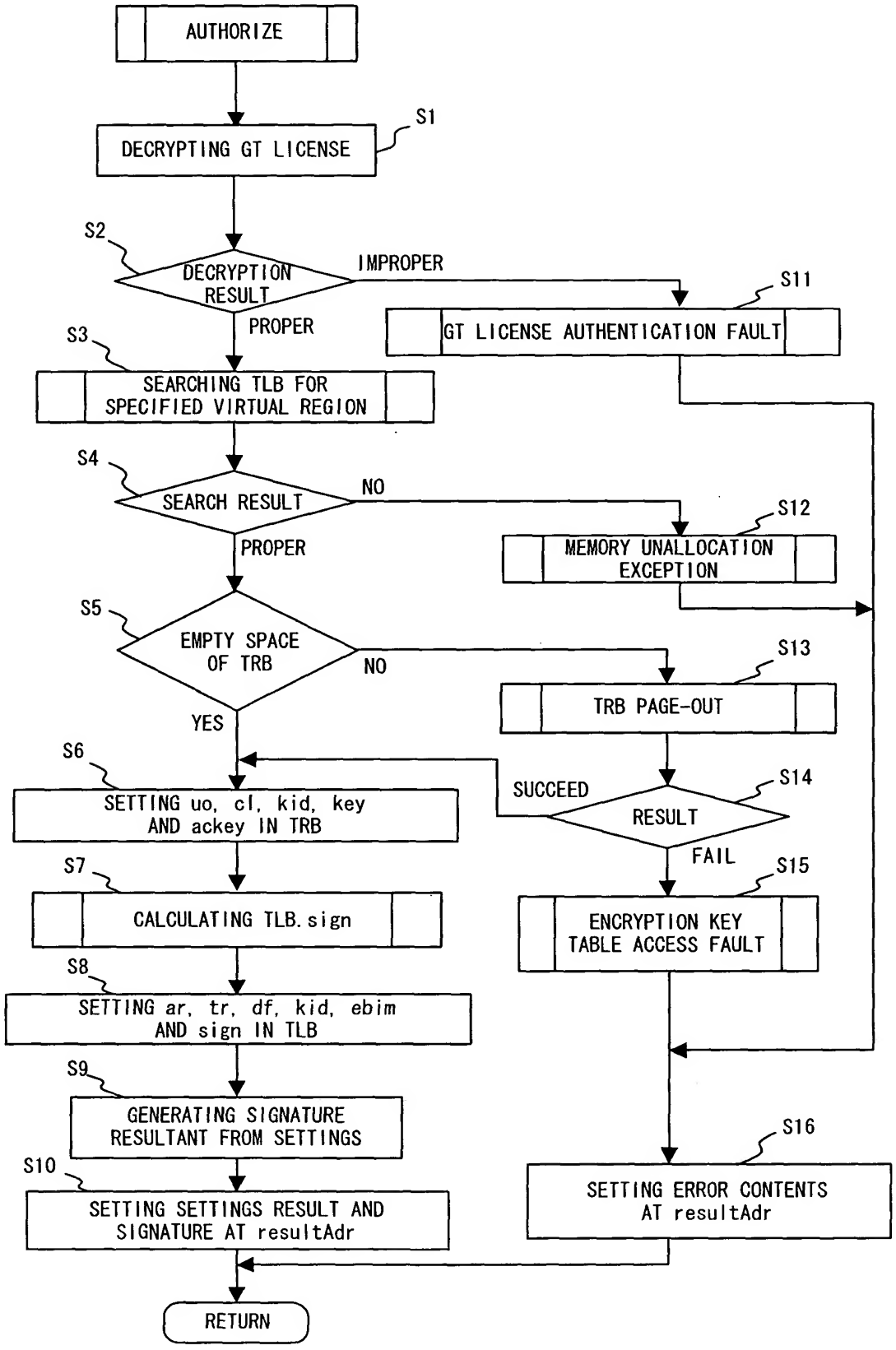

AUTHORIZE
S1
DECRYPTING GT LICENSE
S2
DECRYPTION RESULT
IMPROPER
S11
GT LICENSE AUTHENTICATION FAULT
PROPER
S3
SEARCHING TLB FOR SPECIFIED VIRTUAL REGION
S4
SEARCH RESULT
NO
S12
MEMORY UNALLOCATION EXCEPTION
PROPER
S5
EMPTY SPACE OF TRB
NO
S13
TRB PAGE-OUT
YES
S6
SETTING uo, cl, kid, key AND ackey IN TRB
SUCCEED
S14
RESULT
FAIL
S7
CALCULATING TLB.sign
S15
ENCRYPTION KEY TABLE ACCESS FAULT
S8
SETTING ar, tr, df, kid, ebim AND sign IN TLB
S9
GENERATING SIGNATURE RESULTANT FROM SETTINGS
S16
S10
SETTING SETTINGS RESULT AND SIGNATURE AT resultAdr
SETTING ERROR CONTENTS AT resultAdr
RETURN

FIG. 18

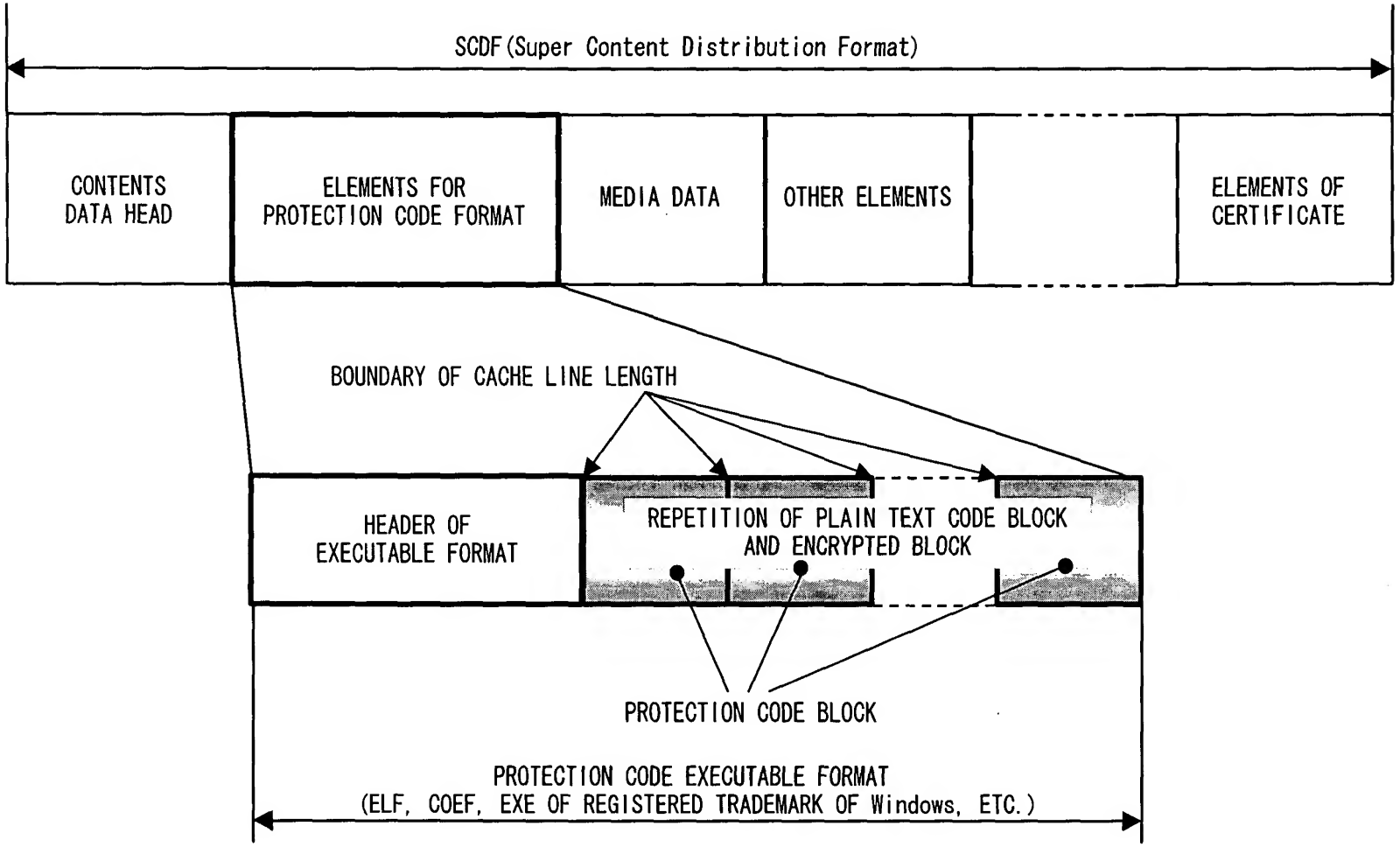

SCDF(Super Content Distribution Format)
CONTENTS DATA HEAD
ELEMENTS FOR PROTECTION CODE FORMAT
MEDIA DATA
OTHER ELEMENTS
ELEMENTS OF CERTIFICATE
BOUNDARY OF CACHE LINE LENGTH
HEADER OF EXECUTABLE FORMAT
REPETITION OF PLAIN TEXT CODE BLOCK AND ENCRYPTED BLOCK
PROTECTION CODE BLOCK
PROTECTION CODE EXECUTABLE FORMAT
(ELF, COEF, EXE OF REGISTERED TRADEMARK OF Windows, ETC.)

FIG. 19

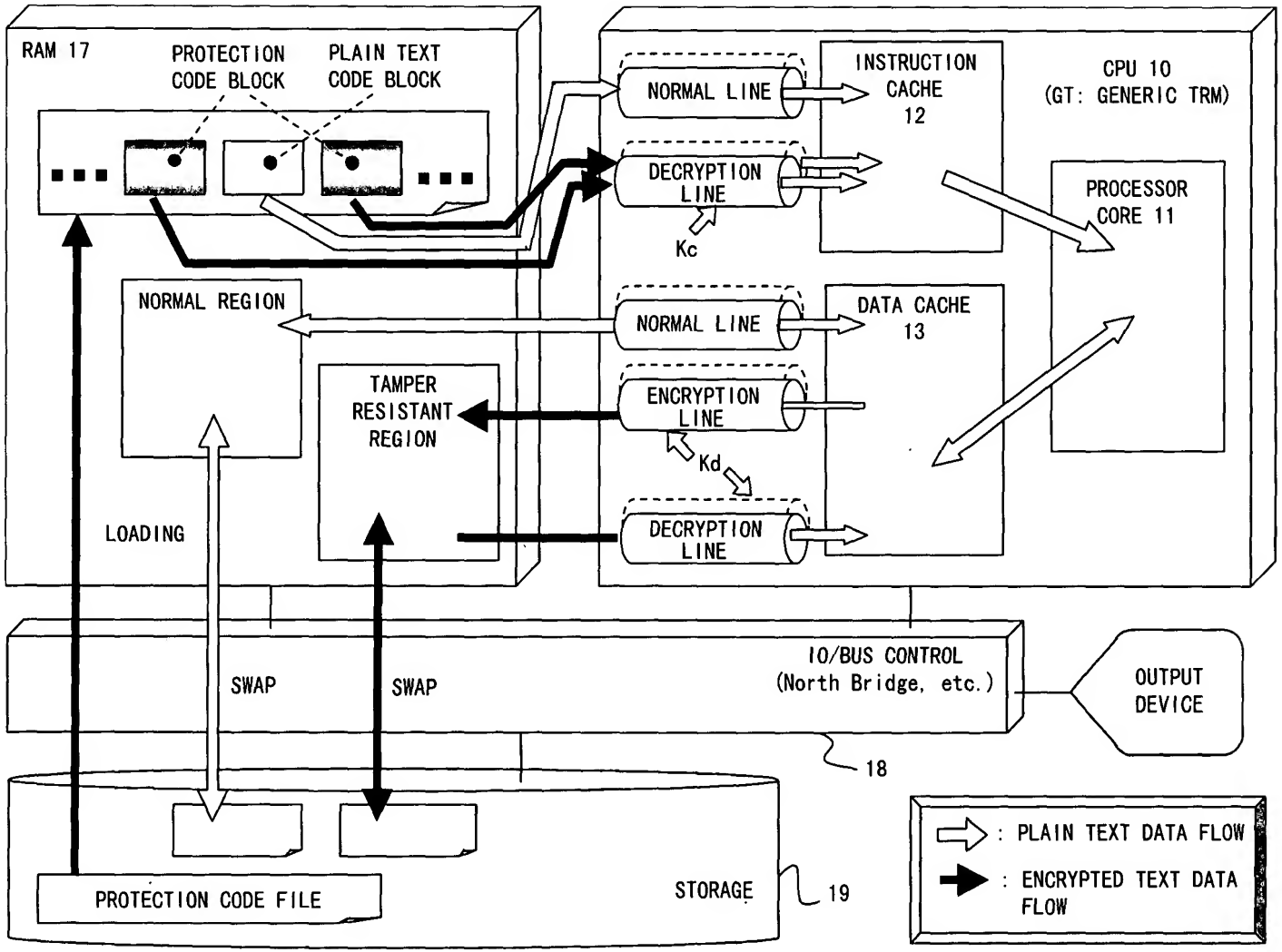

RAM 17
PROTECTION CODE BLOCK
PLAIN TEXT CODE BLOCK
NORMAL REGION
TAMPER RESISTANT REGION
LOADING
SWAP
SWAP
NORMAL LINE
DECRYPTION LINE
Kc
NORMAL LINE
ENCRYPTION LINE
Kd
DECRYPTION LINE
INSTRUCTION CACHE 12
DATA CACHE 13
CPU 10 (GT: GENERIC TRM)
PROCESSOR CORE 11
IO/BUS CONTROL (North Bridge, etc.)
OUTPUT DEVICE
18
PROTECTION CODE FILE
STORAGE
19
: PLAIN TEXT DATA FLOW
: ENCRYPTED TEXT DATA FLOW

FIG. 20

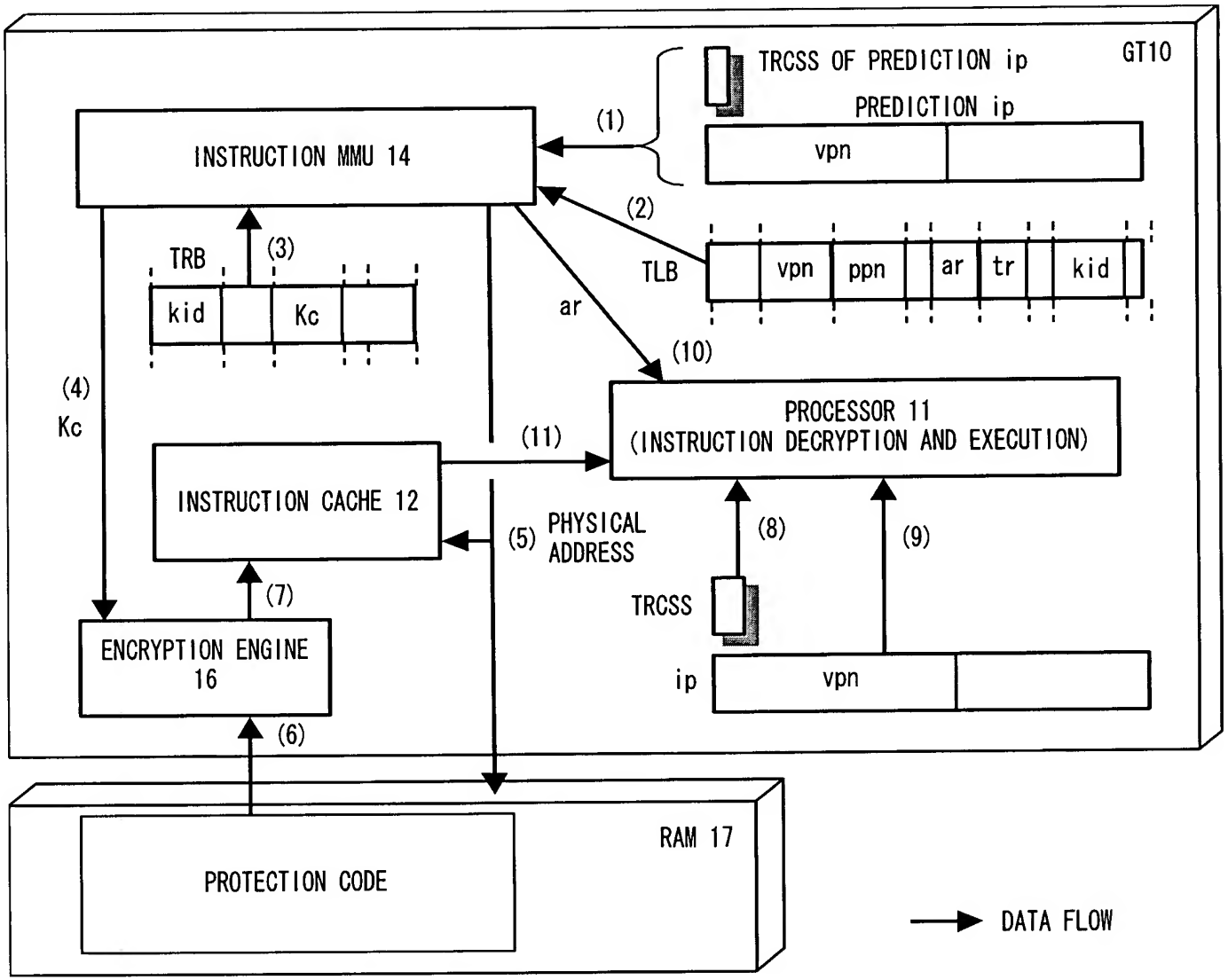

GT10
TRCSS OF PREDICTION ip
PREDICTION ip
vpn
(1)
INSTRUCTION MMU 14
(2)
TLB
vpn
ppn
ar
tr
kid
TRB
(3)
kid
Kc
ar
(10)
(4)
Kc
PROCESSOR 11
(INSTRUCTION DECRYPTION AND EXECUTION)
(11)
INSTRUCTION CACHE 12
(5)
PHYSICAL
ADDRESS
(8)
(9)
TRCSS
(7)
ENCRYPTION ENGINE
16
ip
vpn
(6)
RAM 17
PROTECTION CODE
DATA FLOW

FIG. 21

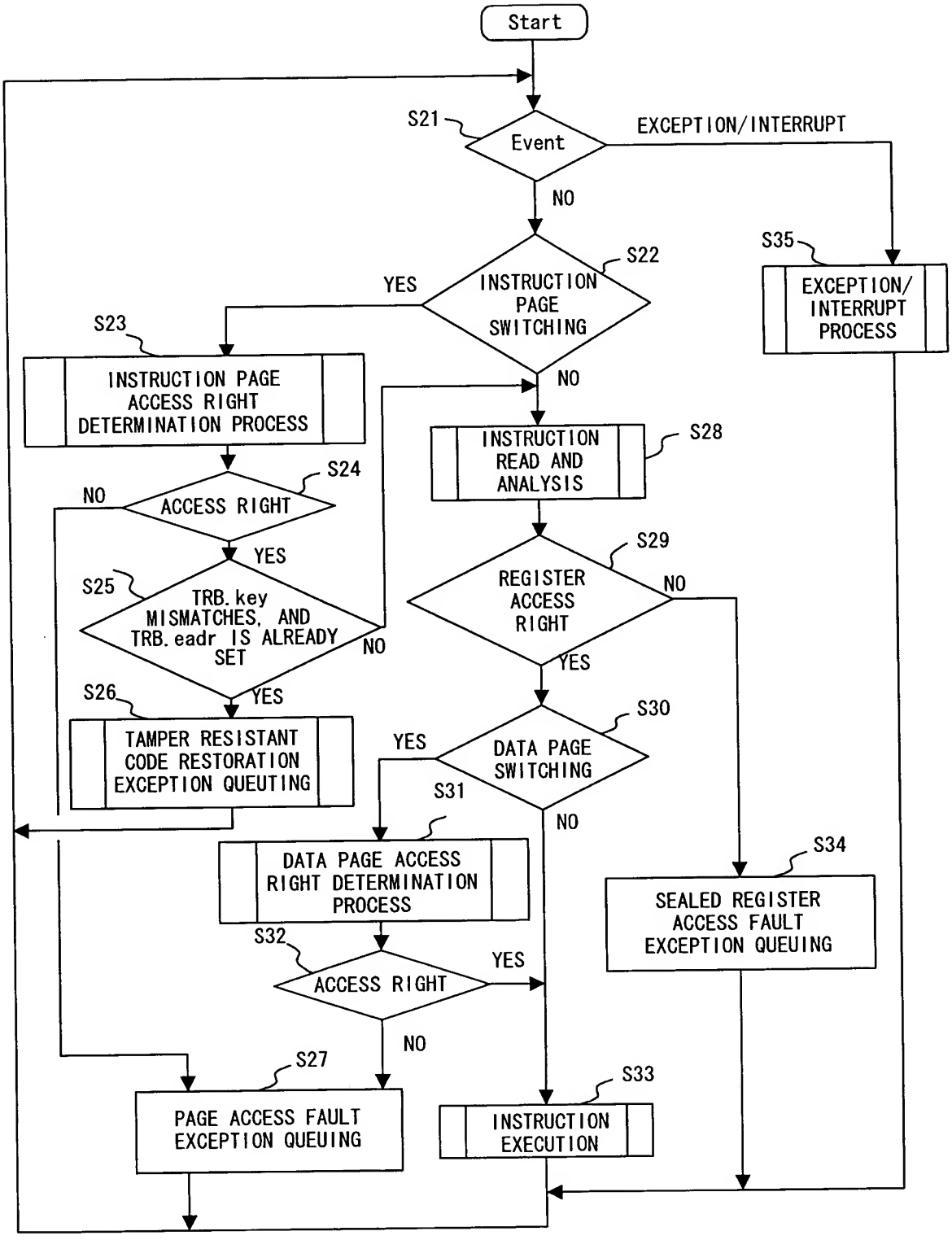

Start
S21
Event
EXCEPTION/INTERRUPT
NO
S22
INSTRUCTION PAGE SWITCHING
YES
S35
EXCEPTION/ INTERRUPT PROCESS
S23
INSTRUCTION PAGE ACCESS RIGHT DETERMINATION PROCESS
NO
S28
INSTRUCTION READ AND ANALYSIS
S24
ACCESS RIGHT
NO
YES
S25
TRB.key MISMATCHES, AND TRB.eadr IS ALREADY SET
NO
YES
S29
REGISTER ACCESS RIGHT
NO
YES
S26
TAMPER RESISTANT CODE RESTORATION EXCEPTION QUEUTING
S30
DATA PAGE SWITCHING
YES
NO
S31
DATA PAGE ACCESS RIGHT DETERMINATION PROCESS
S34
SEALED REGISTER ACCESS FAULT EXCEPTION QUEUING
S32
ACCESS RIGHT
YES
NO
S27
PAGE ACCESS FAULT EXCEPTION QUEUING
S33
INSTRUCTION EXECUTION

FIG. 22

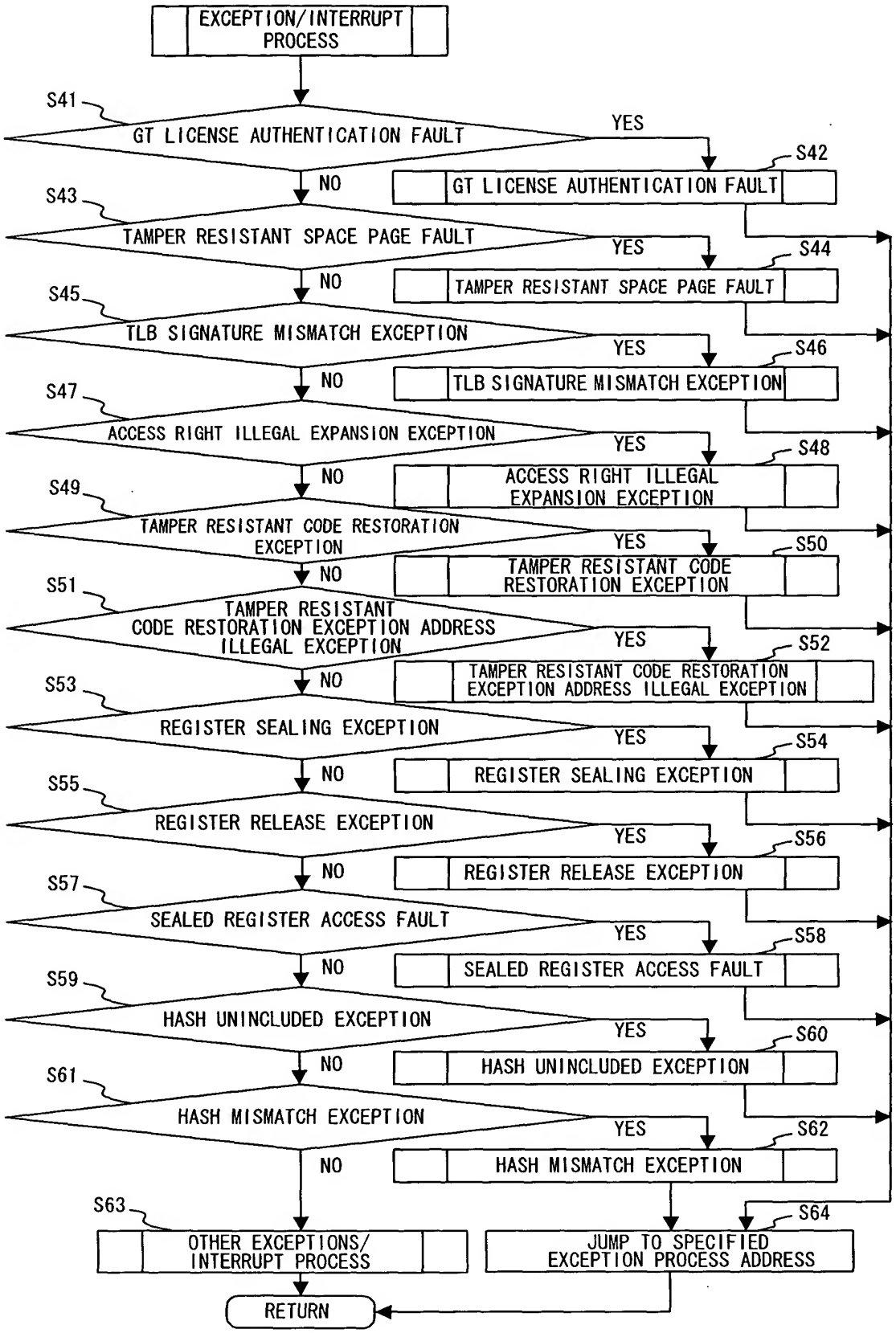

EXCEPTION/INTERRUPT PROCESS
S41
GT LICENSE AUTHENTICATION FAULT
YES
S42
GT LICENSE AUTHENTICATION FAULT
NO
S43
TAMPER RESISTANT SPACE PAGE FAULT
YES
S44
TAMPER RESISTANT SPACE PAGE FAULT
NO
S45
TLB SIGNATURE MISMATCH EXCEPTION
YES
S46
TLB SIGNATURE MISMATCH EXCEPTION
NO
S47
ACCESS RIGHT ILLEGAL EXPANSION EXCEPTION
YES
S48
ACCESS RIGHT ILLEGAL EXPANSION EXCEPTION
NO
S49
TAMPER RESISTANT CODE RESTORATION EXCEPTION
YES
S50
TAMPER RESISTANT CODE RESTORATION EXCEPTION
NO
S51
TAMPER RESISTANT CODE RESTORATION EXCEPTION ADDRESS ILLEGAL EXCEPTION
YES
S52
TAMPER RESISTANT CODE RESTORATION EXCEPTION ADDRESS ILLEGAL EXCEPTION
NO
S53
REGISTER SEALING EXCEPTION
YES
S54
REGISTER SEALING EXCEPTION
NO
S55
REGISTER RELEASE EXCEPTION
YES
S56
REGISTER RELEASE EXCEPTION
NO
S57
SEALED REGISTER ACCESS FAULT
YES
S58
SEALED REGISTER ACCESS FAULT
NO
S59
HASH UNINCLUDED EXCEPTION
YES
S60
HASH UNINCLUDED EXCEPTION
NO
S61
HASH MISMATCH EXCEPTION
YES
S62
HASH MISMATCH EXCEPTION
NO
S63
OTHER EXCEPTIONS/ INTERRUPT PROCESS
S64
JUMP TO SPECIFIED EXCEPTION PROCESS ADDRESS
RETURN

FIG. 23

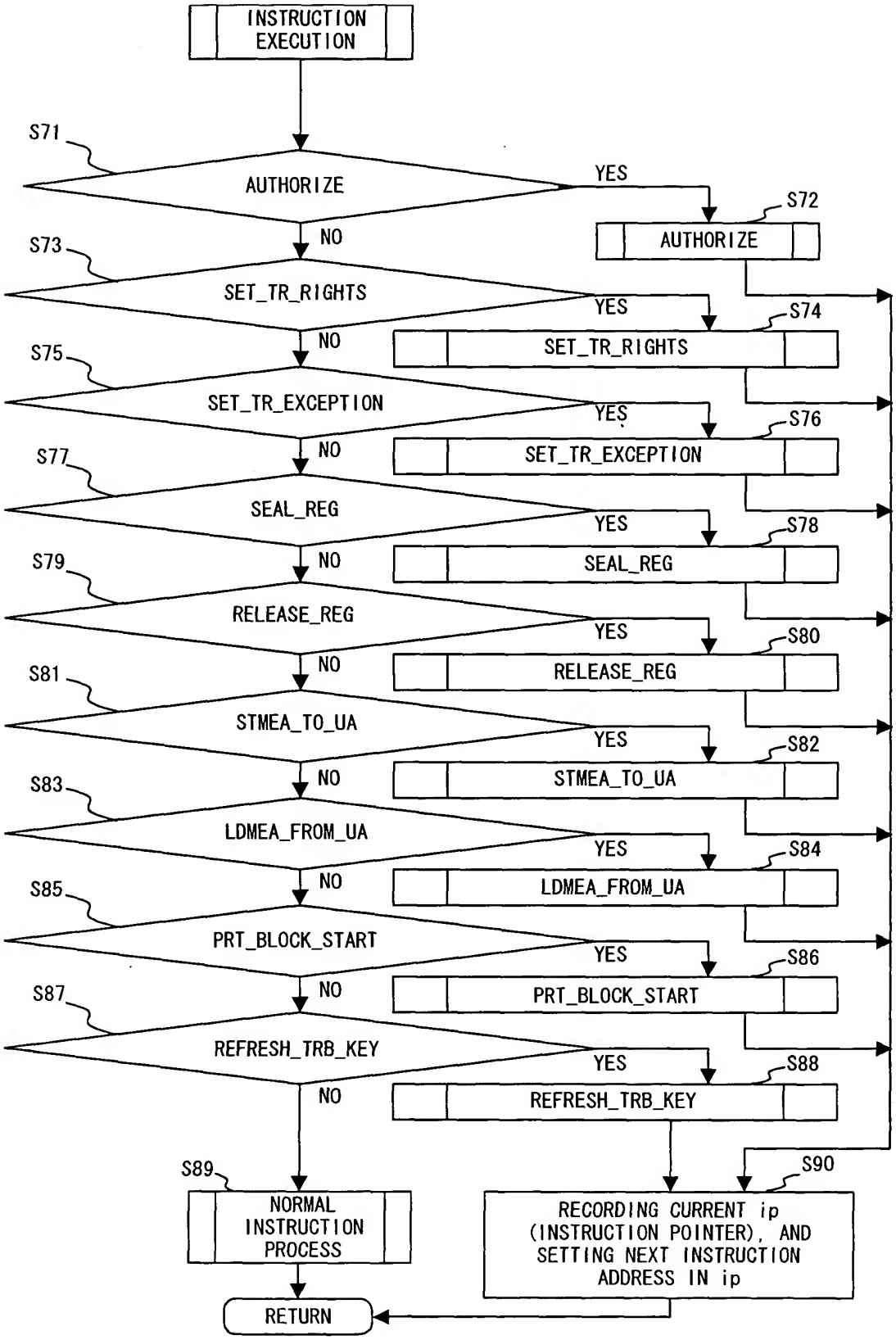

INSTRUCTION EXECUTION
S71
AUTHORIZE
YES
S72
AUTHORIZE
NO
S73
SET_TR_RIGHTS
YES
S74
SET_TR_RIGHTS
NO
S75
SET_TR_EXCEPTION
YES
S76
SET_TR_EXCEPTION
NO
S77
SEAL_REG
YES
S78
SEAL_REG
NO
S79
RELEASE_REG
YES
S80
RELEASE_REG
NO
S81
STMEA_TO_UA
YES
S82
STMEA_TO_UA
NO
S83
LDMEA_FROM_UA
YES
S84
LDMEA_FROM_UA
NO
S85
PRT_BLOCK_START
YES
S86
PRT_BLOCK_START
NO
S87
REFRESH_TRB_KEY
YES
S88
REFRESH_TRB_KEY
NO
S89
NORMAL INSTRUCTION PROCESS
S90
RECORDING CURRENT ip (INSTRUCTION POINTER), AND SETTING NEXT INSTRUCTION ADDRESS IN ip
RETURN

FIG. 24

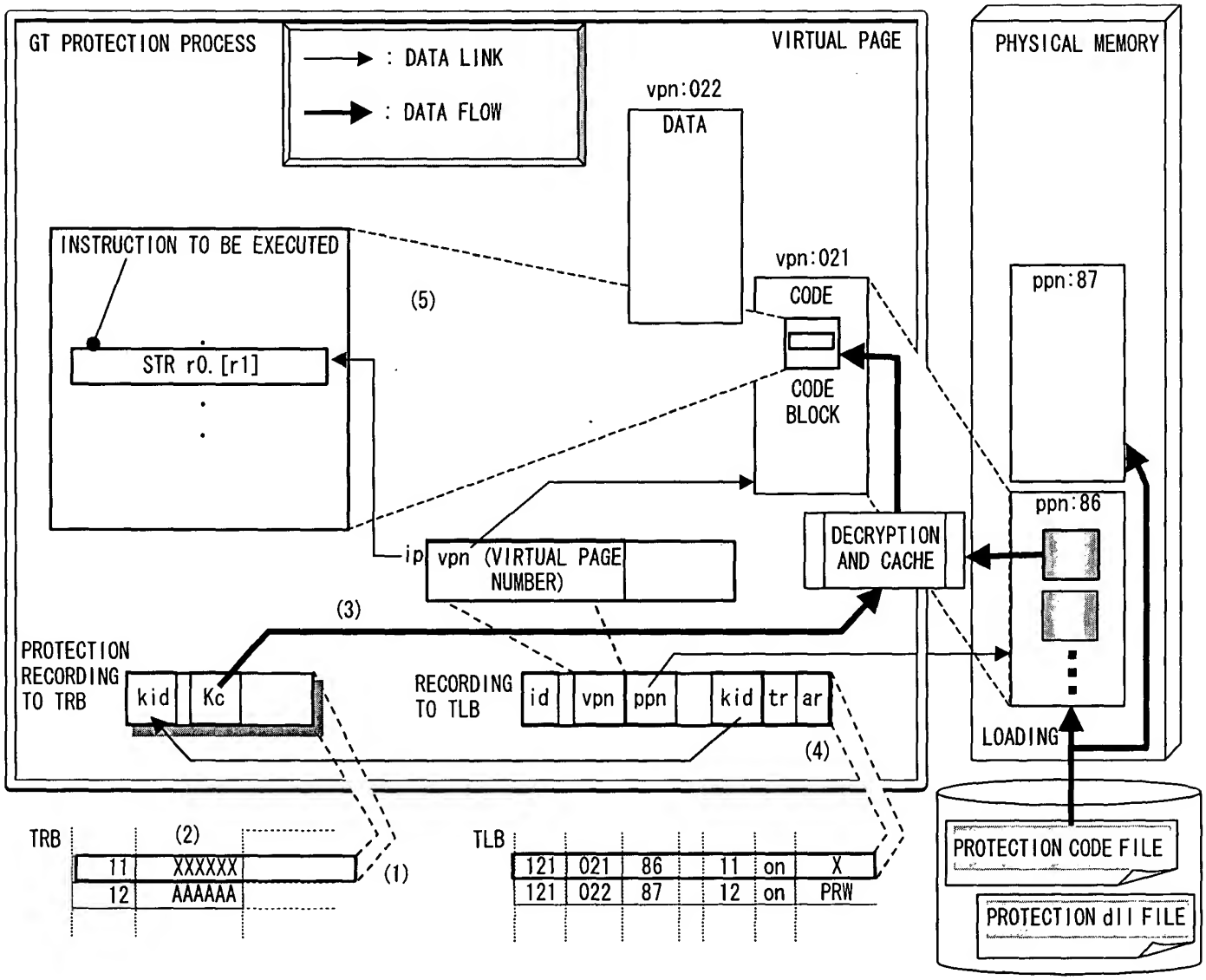

GT PROTECTION PROCESS
: DATA LINK
: DATA FLOW
VIRTUAL PAGE
vpn:022
DATA
PHYSICAL MEMORY
INSTRUCTION TO BE EXECUTED
(5)
vpn:021
CODE
ppn:87
STR r0. [r1]
CODE BLOCK
ppn:86
DECRYPTION AND CACHE
ip
vpn (VIRTUAL PAGE NUMBER)
(3)
PROTECTION RECORDING TO TRB
kid
Kc
RECORDING TO TLB
id
vpn
ppn
kid
tr
ar
(4)
LOADING
TRB
(2)
11
XXXXXX
12
AAAAAA
(1)
TLB
121
021
86
11
on
X
121
022
87
12
on
PRW
PROTECTION CODE FILE
PROTECTION dll FILE

FIG. 25

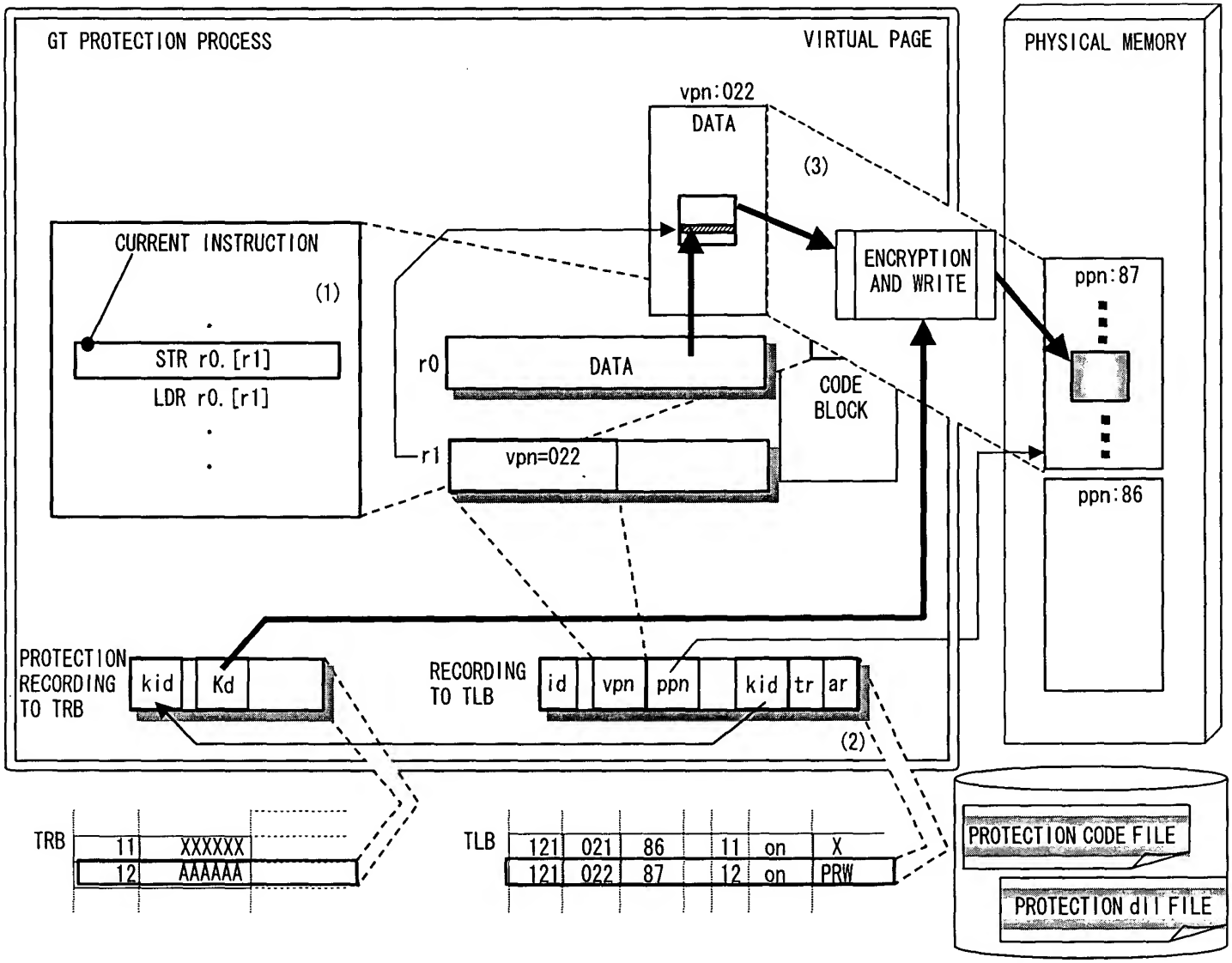

GT PROTECTION PROCESS
VIRTUAL PAGE
PHYSICAL MEMORY
vpn:022
DATA
(3)
CURRENT INSTRUCTION
(1)
STR r0. [r1]
LDR r0. [r1]
r0
DATA
r1
vpn=022
CODE BLOCK
ENCRYPTION AND WRITE
ppn:87
ppn:86
PROTECTION RECORDING TO TRB
kid
Kd
RECORDING TO TLB
id
vpn
ppn
kid
tr
ar
(2)
TRB
11 XXXXXX
12 AAAAAA
TLB
121 021 86 11 on X
121 022 87 12 on PRW
PROTECTION CODE FILE
PROTECTION dll FILE

FIG. 26

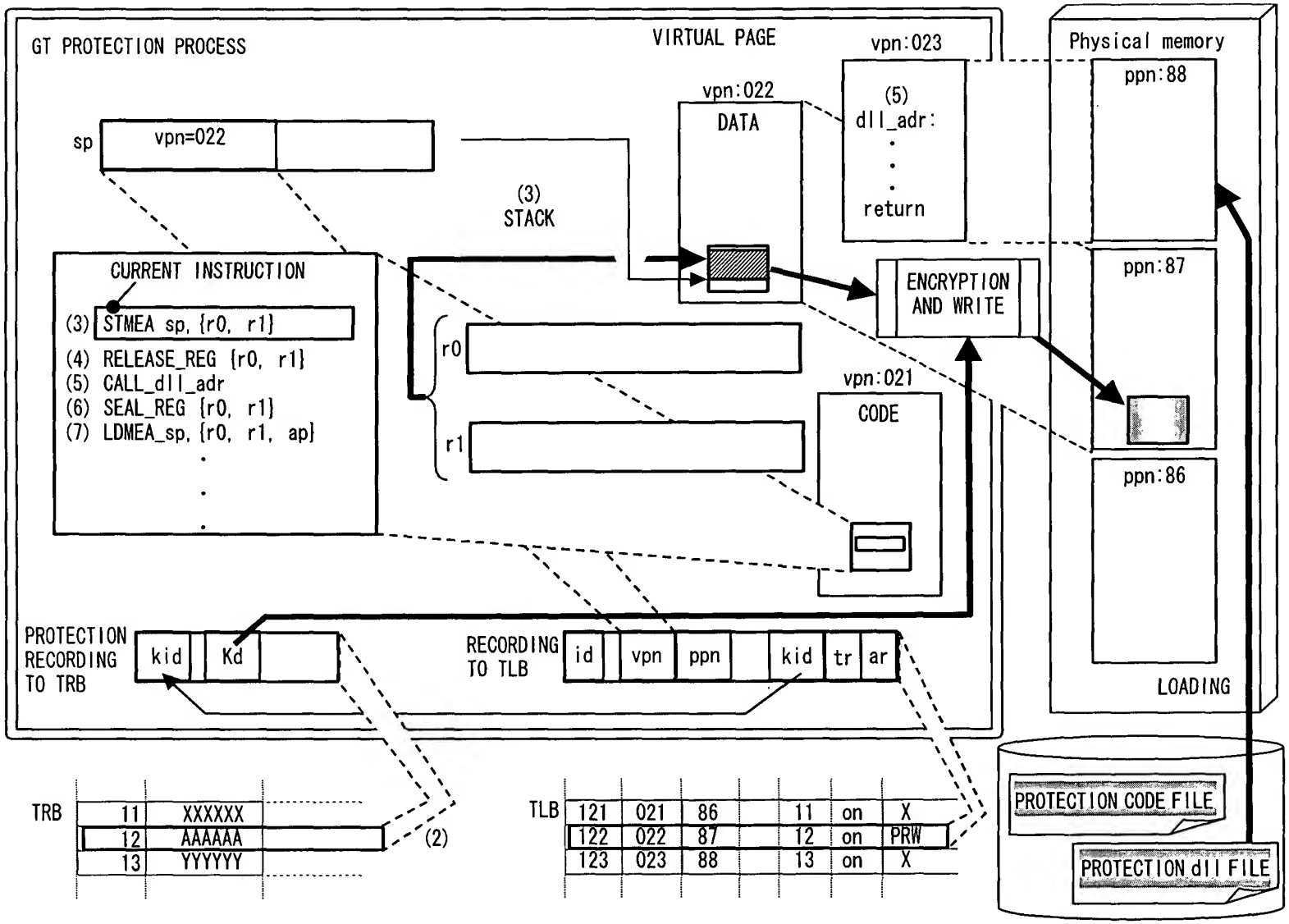

GT PROTECTION PROCESS
VIRTUAL PAGE
vpn:023
vpn:022
DATA
(5)
dll_adr:
return
Physical memory
ppn:88
ppn:87
ppn:86
sp
vpn=022
(3)
STACK
CURRENT INSTRUCTION
(3) STMEA sp, {r0, r1}
(4) RELEASE_REG {r0, r1}
(5) CALL_dll_adr
(6) SEAL_REG {r0, r1}
(7) LDMEA_sp, {r0, r1, ap}
r0
r1
ENCRYPTION
AND WRITE
vpn:021
CODE
PROTECTION
RECORDING
TO TRB
kid
Kd
RECORDING
TO TLB
id
vpn
ppn
kid
tr
ar
LOADING
TRB
11 XXXXXX
12 AAAAAA
13 YYYYYY
(2)
TLB
121 021 86 11 on X
122 022 87 12 on PRW
123 023 88 13 on X
PROTECTION CODE FILE
PROTECTION dll FILE

FIG. 27

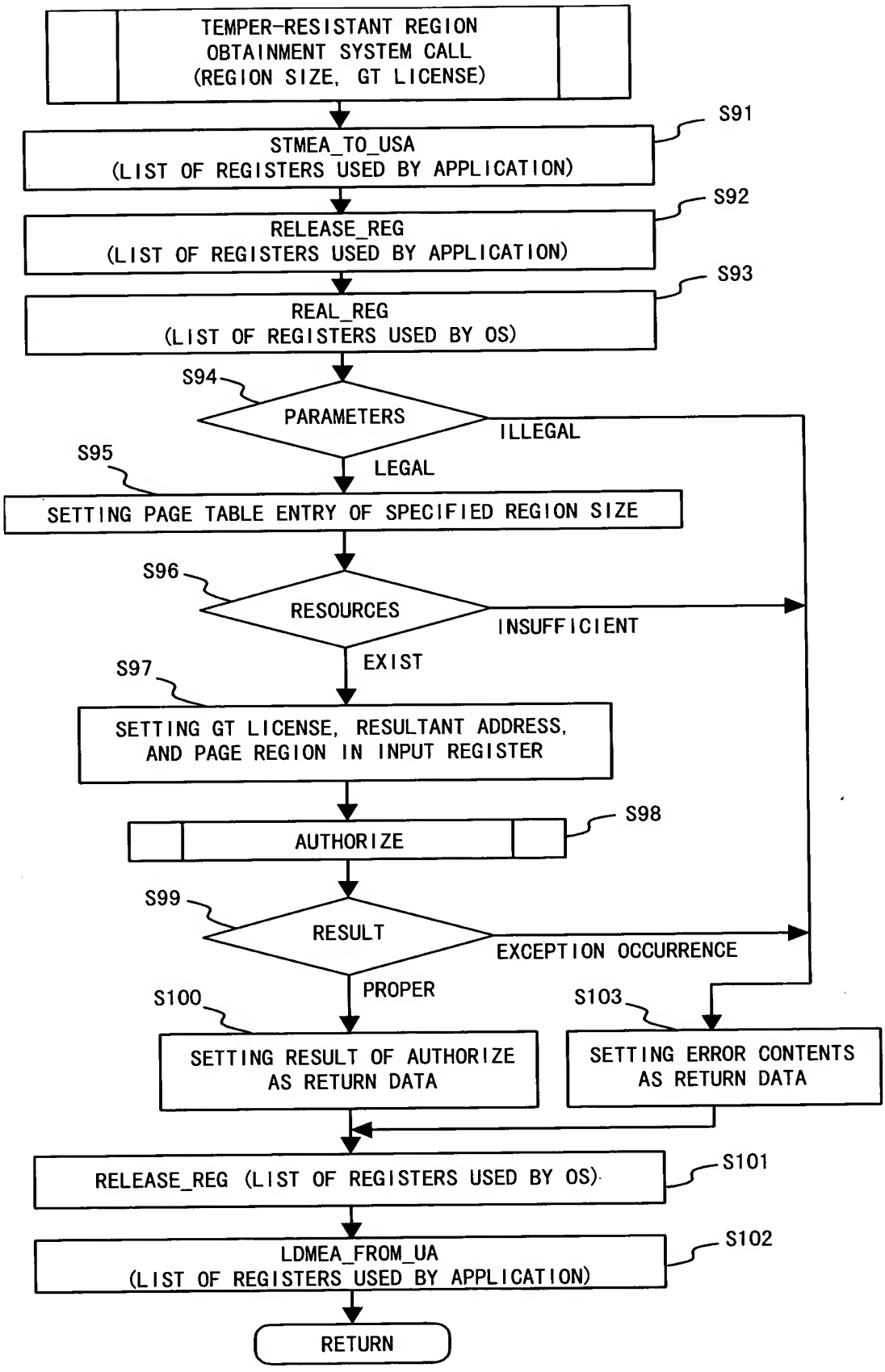

TEMPER-RESISTANT REGION OBTAINMENT SYSTEM CALL (REGION SIZE, GT LICENSE)
S91
STMEA_TO_USA (LIST OF REGISTERS USED BY APPLICATION)
S92
RELEASE_REG (LIST OF REGISTERS USED BY APPLICATION)
S93
REAL_REG (LIST OF REGISTERS USED BY OS)
S94
PARAMETERS
ILLEGAL
LEGAL
S95
SETTING PAGE TABLE ENTRY OF SPECIFIED REGION SIZE
S96
RESOURCES
INSUFFICIENT
EXIST
S97
SETTING GT LICENSE, RESULTANT ADDRESS, AND PAGE REGION IN INPUT REGISTER
S98
AUTHORIZE
S99
RESULT
EXCEPTION OCCURRENCE
PROPER
S100
SETTING RESULT OF AUTHORIZE AS RETURN DATA
S103
SETTING ERROR CONTENTS AS RETURN DATA
S101
RELEASE_REG (LIST OF REGISTERS USED BY OS)
S102
LDMEA_FROM_UA (LIST OF REGISTERS USED BY APPLICATION)
RETURN

FIG. 28

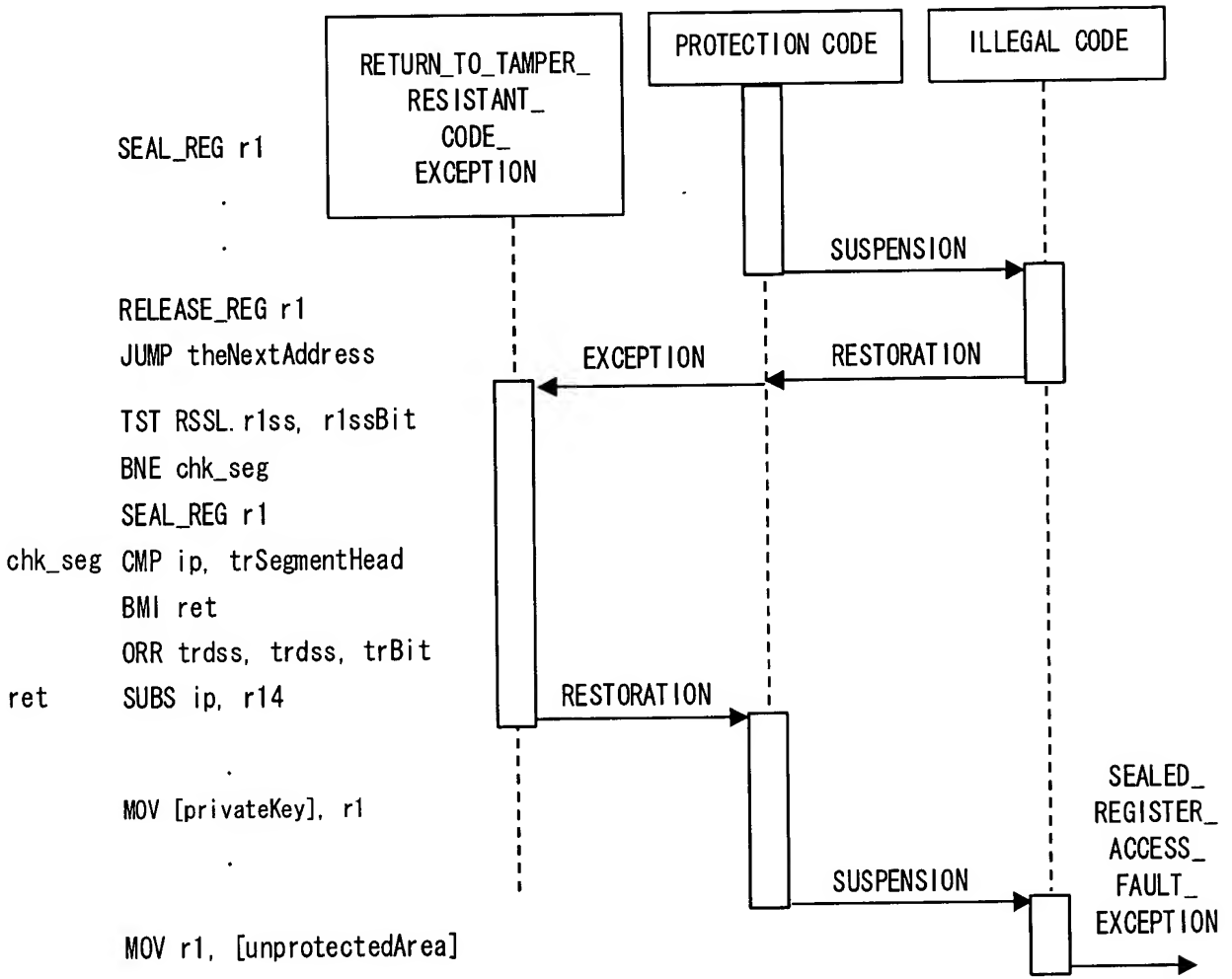

RETURN_TO_TAMPER_
RESISTANT_
CODE_
EXCEPTION
PROTECTION CODE
ILLEGAL CODE
SEAL_REG r1
SUSPENSION
RELEASE_REG r1
JUMP theNextAddress
EXCEPTION
RESTORATION
TST RSSL.r1ss, r1ssBit
BNE chk_seg
SEAL_REG r1
chk_seg CMP ip, trSegmentHead
BMI ret
ORR trdss, trdss, trBit
ret SUBS ip, r14
RESTORATION
MOV [privateKey], r1
SUSPENSION
SEALED_
REGISTER_
ACCESS_
FAULT_
EXCEPTION
MOV r1, [unprotectedArea]

FIG. 29

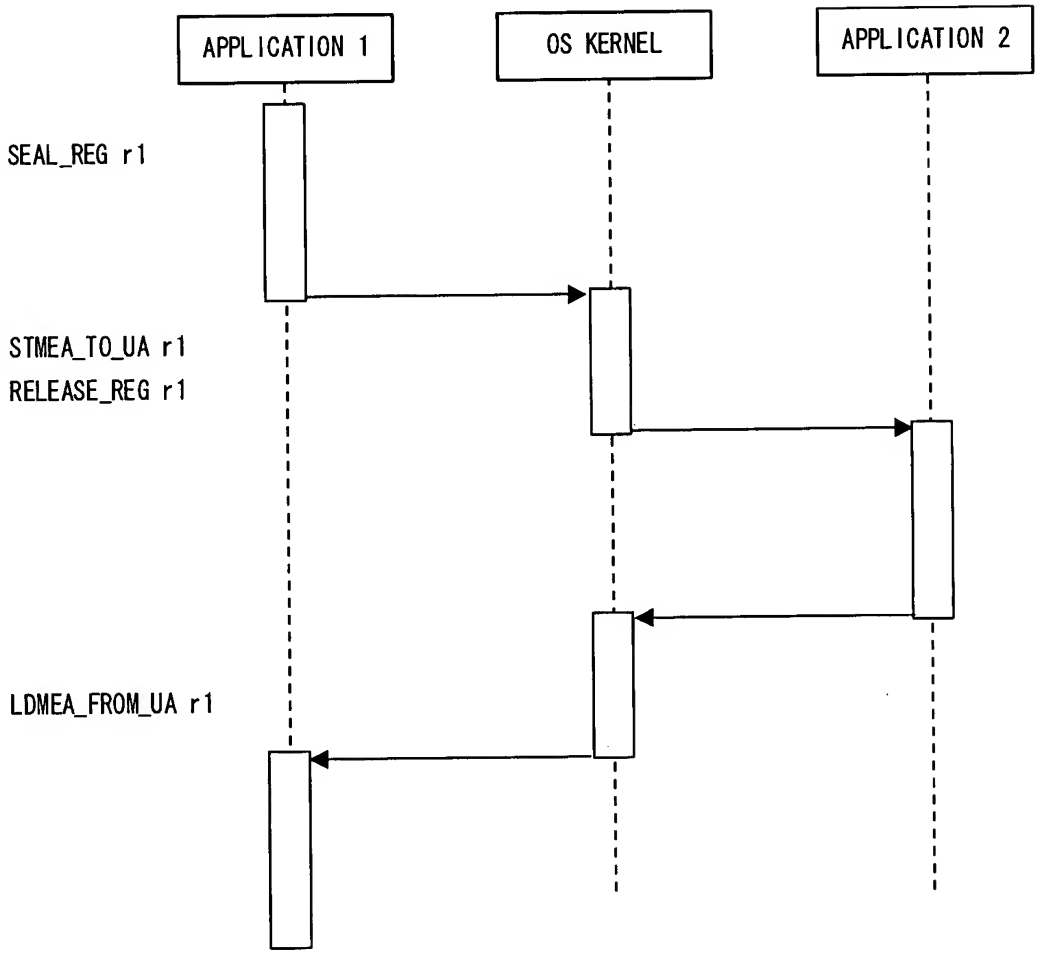

APPLICATION 1
OS KERNEL
APPLICATION 2
SEAL_REG r1
STMEA_TO_UA r1
RELEASE_REG r1
LDMEA_FROM_UA r1

FIG. 30

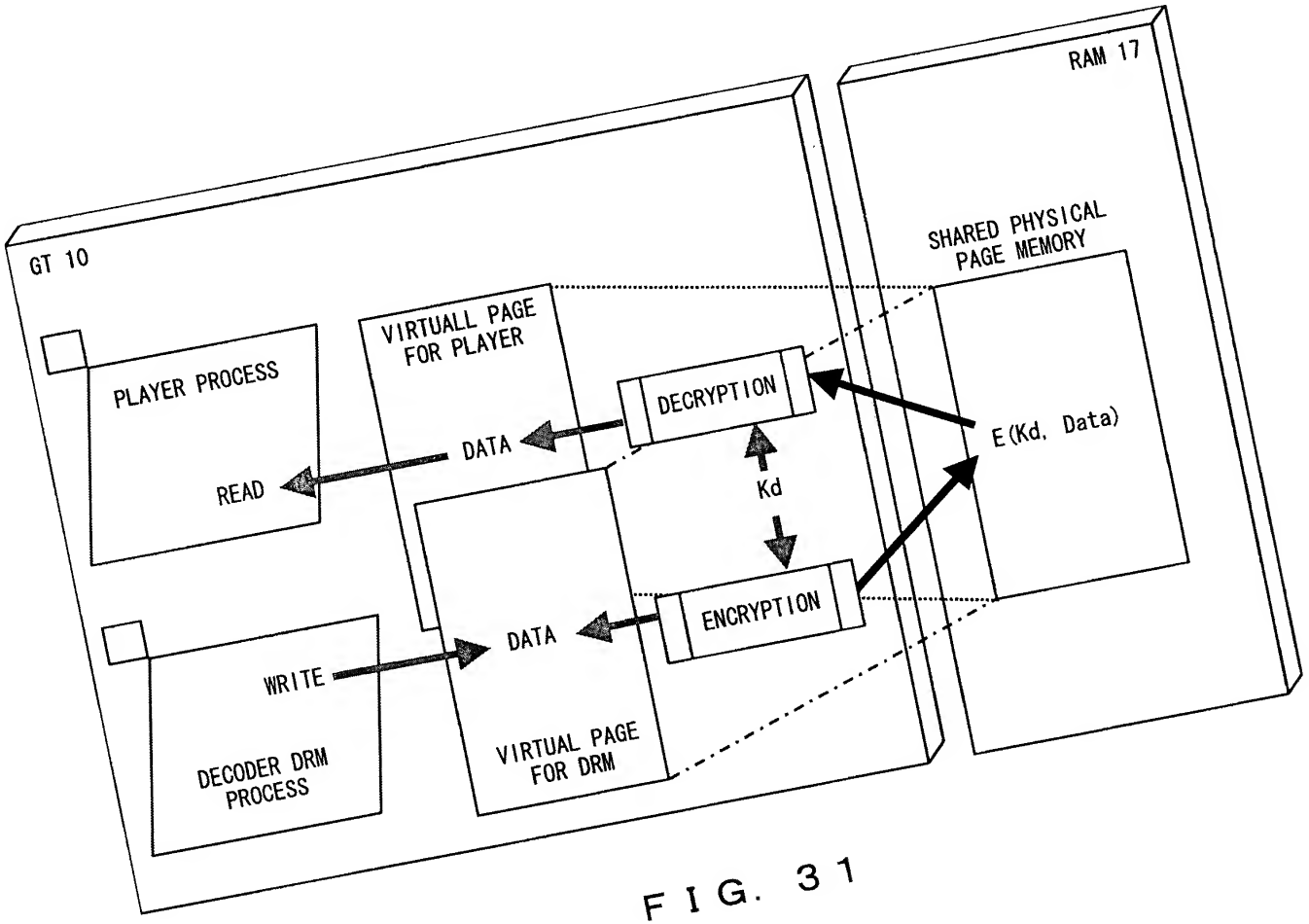

RAM 17
GT 10
SHARED PHYSICAL PAGE MEMORY
PLAYER PROCESS
VIRTUALL PAGE FOR PLAYER
DECRYPTION
DATA
READ
Kd
E(Kd, Data)
ENCRYPTION
DATA
WRITE
DECODER DRM PROCESS
VIRTUAL PAGE FOR DRM

FIG. 31

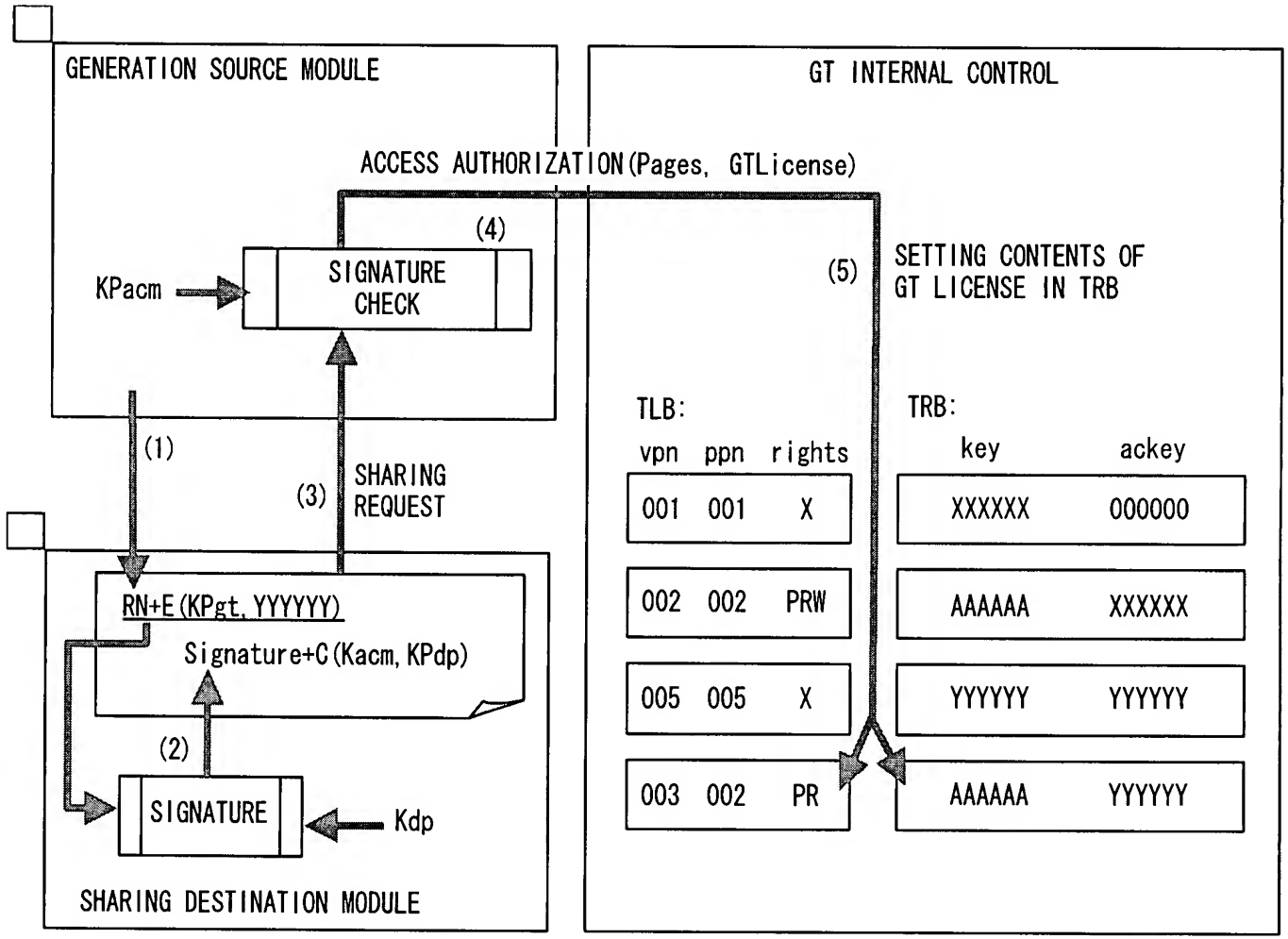

GENERATION SOURCE MODULE
GT INTERNAL CONTROL
ACCESS AUTHORIZATION(Pages, GTLicense)
(4)
KPacm
SIGNATURE CHECK
(5)
SETTING CONTENTS OF GT LICENSE IN TRB
TLB:
vpn ppn rights
001 001 X
002 002 PRW
005 005 X
003 002 PR
TRB:
key ackey
XXXXXX 000000
AAAAAA XXXXXX
YYYYYY YYYYYY
AAAAAA YYYYYY
(1)
(3)
SHARING REQUEST
RN+E(KPgt, YYYYYY)
Signature+C(Kacm, KPdp)
(2)
SIGNATURE
Kdp
SHARING DESTINATION MODULE

FIG. 32

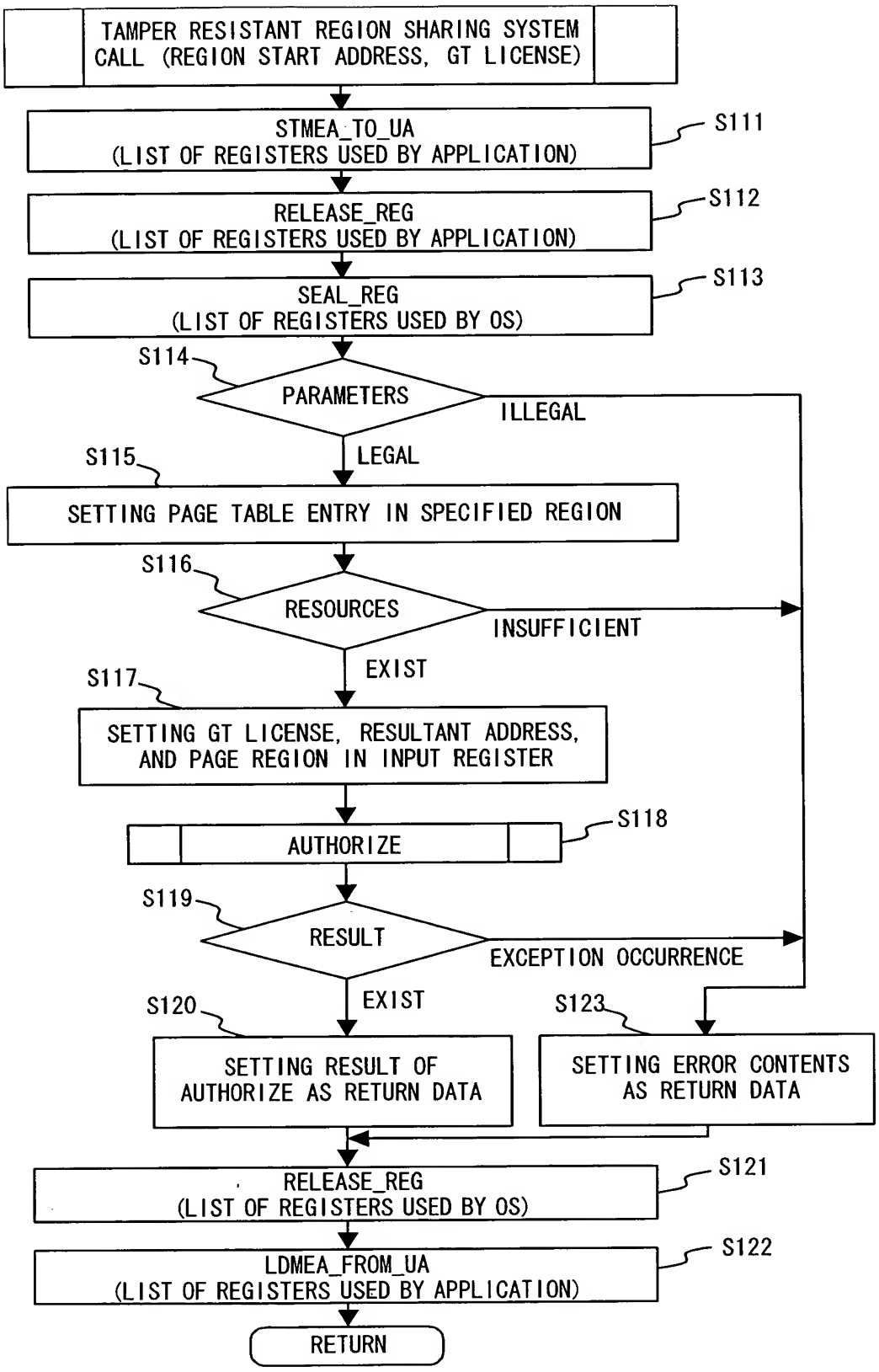

TAMPER RESISTANT REGION SHARING SYSTEM CALL (REGION START ADDRESS, GT LICENSE)
STMEA_TO_UA (LIST OF REGISTERS USED BY APPLICATION)
S111
RELEASE_REG (LIST OF REGISTERS USED BY APPLICATION)
S112
SEAL_REG (LIST OF REGISTERS USED BY OS)
S113
S114
PARAMETERS
ILLEGAL
LEGAL
S115
SETTING PAGE TABLE ENTRY IN SPECIFIED REGION
S116
RESOURCES
INSUFFICIENT
EXIST
S117
SETTING GT LICENSE, RESULTANT ADDRESS, AND PAGE REGION IN INPUT REGISTER
AUTHORIZE
S118
S119
RESULT
EXCEPTION OCCURRENCE
EXIST
S120
SETTING RESULT OF AUTHORIZE AS RETURN DATA
S123
SETTING ERROR CONTENTS AS RETURN DATA
RELEASE_REG (LIST OF REGISTERS USED BY OS)
S121
LDMEA_FROM_UA (LIST OF REGISTERS USED BY APPLICATION)
S122
RETURN

FIG. 33

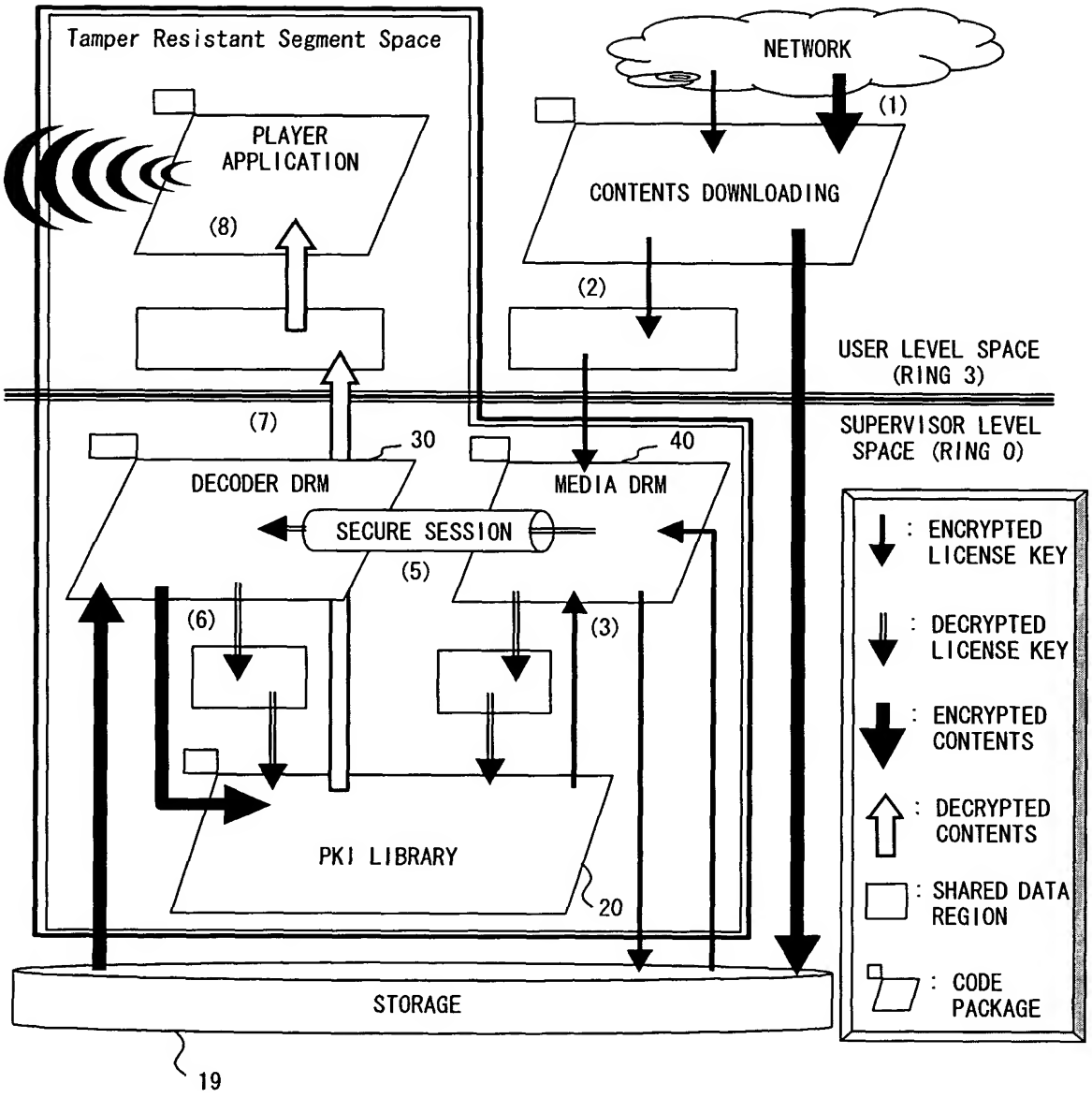

Tamper Resistant Segment Space
NETWORK
(1)
PLAYER APPLICATION
(8)
CONTENTS DOWNLOADING
(2)
USER LEVEL SPACE (RING 3)
SUPERVISOR LEVEL SPACE (RING 0)
(7)
30
40
DECODER DRM
MEDIA DRM
SECURE SESSION
(5)
(6)
(3)
PKI LIBRARY
20
STORAGE
19
: ENCRYPTED LICENSE KEY
: DECRYPTED LICENSE KEY
: ENCRYPTED CONTENTS
: DECRYPTED CONTENTS
: SHARED DATA REGION
: CODE PACKAGE

FIG. 34

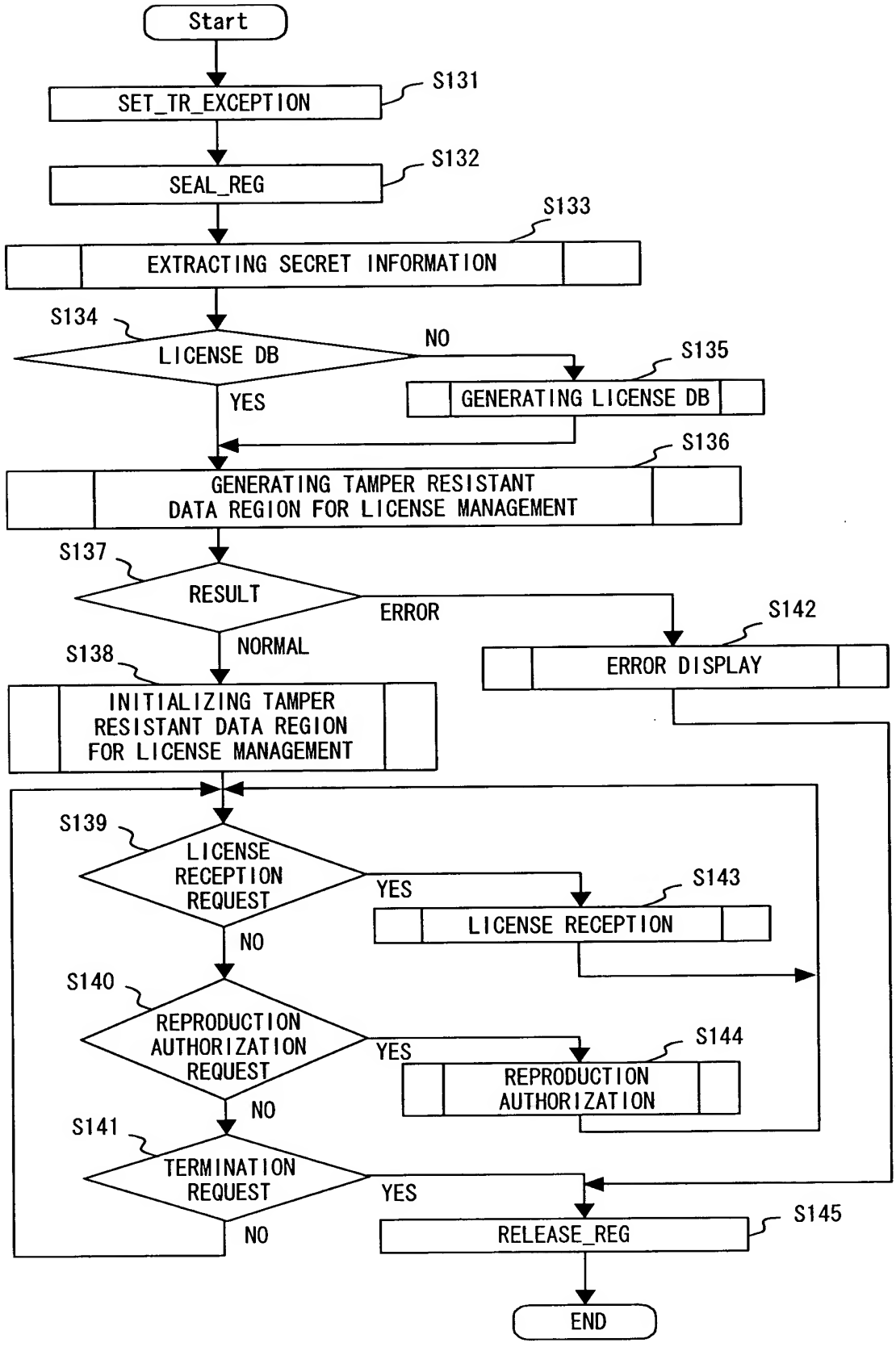

Start
SET_TR_EXCEPTION
S131
SEAL_REG
S132
EXTRACTING SECRET INFORMATION
S133
S134
LICENSE DB
NO
YES
S135
GENERATING LICENSE DB
S136
GENERATING TAMPER RESISTANT DATA REGION FOR LICENSE MANAGEMENT
S137
RESULT
ERROR
NORMAL
S142
ERROR DISPLAY
S138
INITIALIZING TAMPER RESISTANT DATA REGION FOR LICENSE MANAGEMENT
S139
LICENSE RECEPTION REQUEST
YES
S143
LICENSE RECEPTION
NO
S140
REPRODUCTION AUTHORIZATION REQUEST
YES
S144
REPRODUCTION AUTHORIZATION
NO
S141
TERMINATION REQUEST
YES
NO
S145
RELEASE_REG
END

FIG. 35

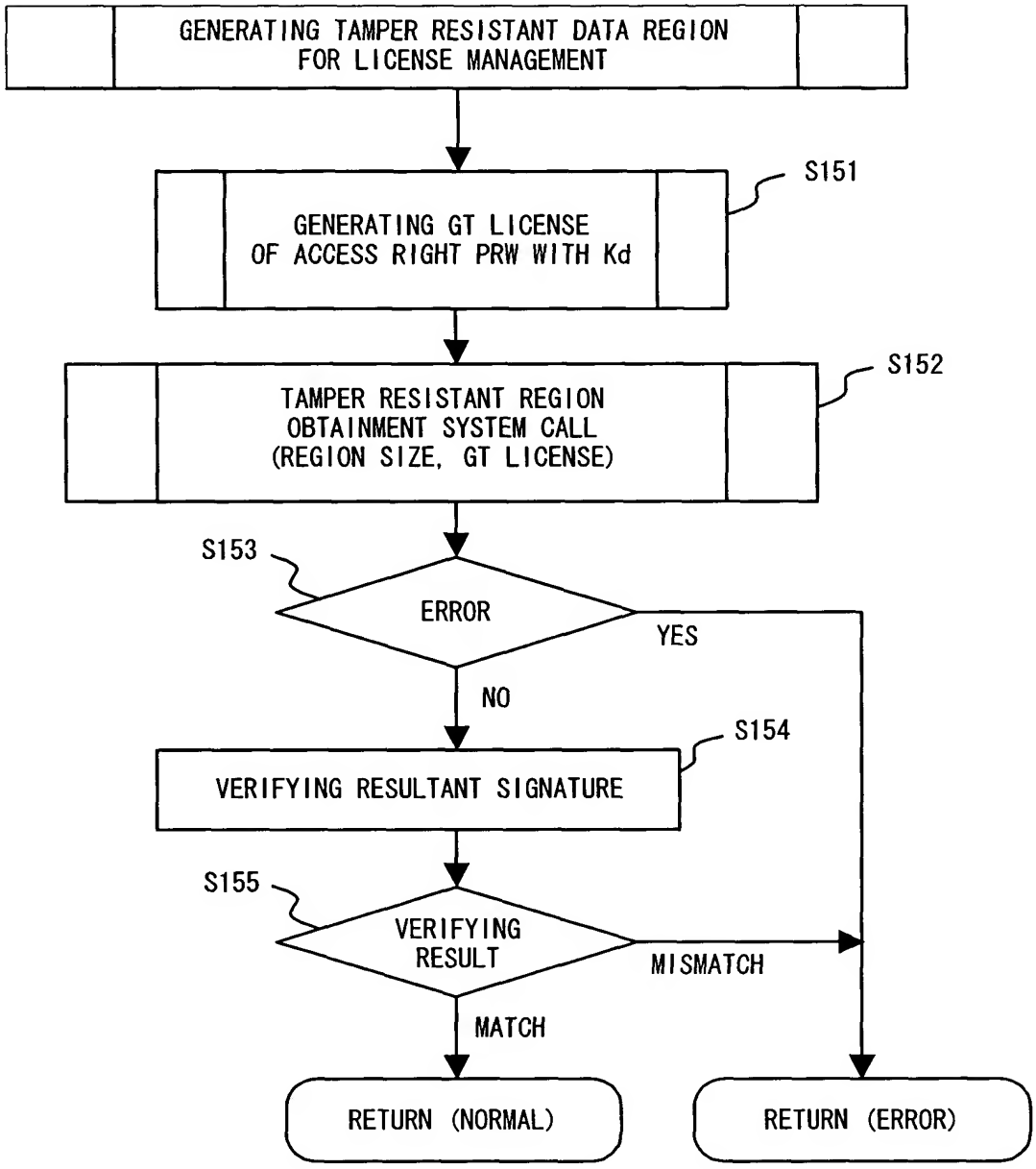

GENERATING TAMPER RESISTANT DATA REGION FOR LICENSE MANAGEMENT
S151
GENERATING GT LICENSE OF ACCESS RIGHT PRW WITH Kd
S152
TAMPER RESISTANT REGION OBTAINMENT SYSTEM CALL (REGION SIZE, GT LICENSE)
S153
ERROR
YES
NO
S154
VERIFYING RESULTANT SIGNATURE
S155
VERIFYING RESULT
MISMATCH
MATCH
RETURN (NORMAL)
RETURN (ERROR)

FIG. 36

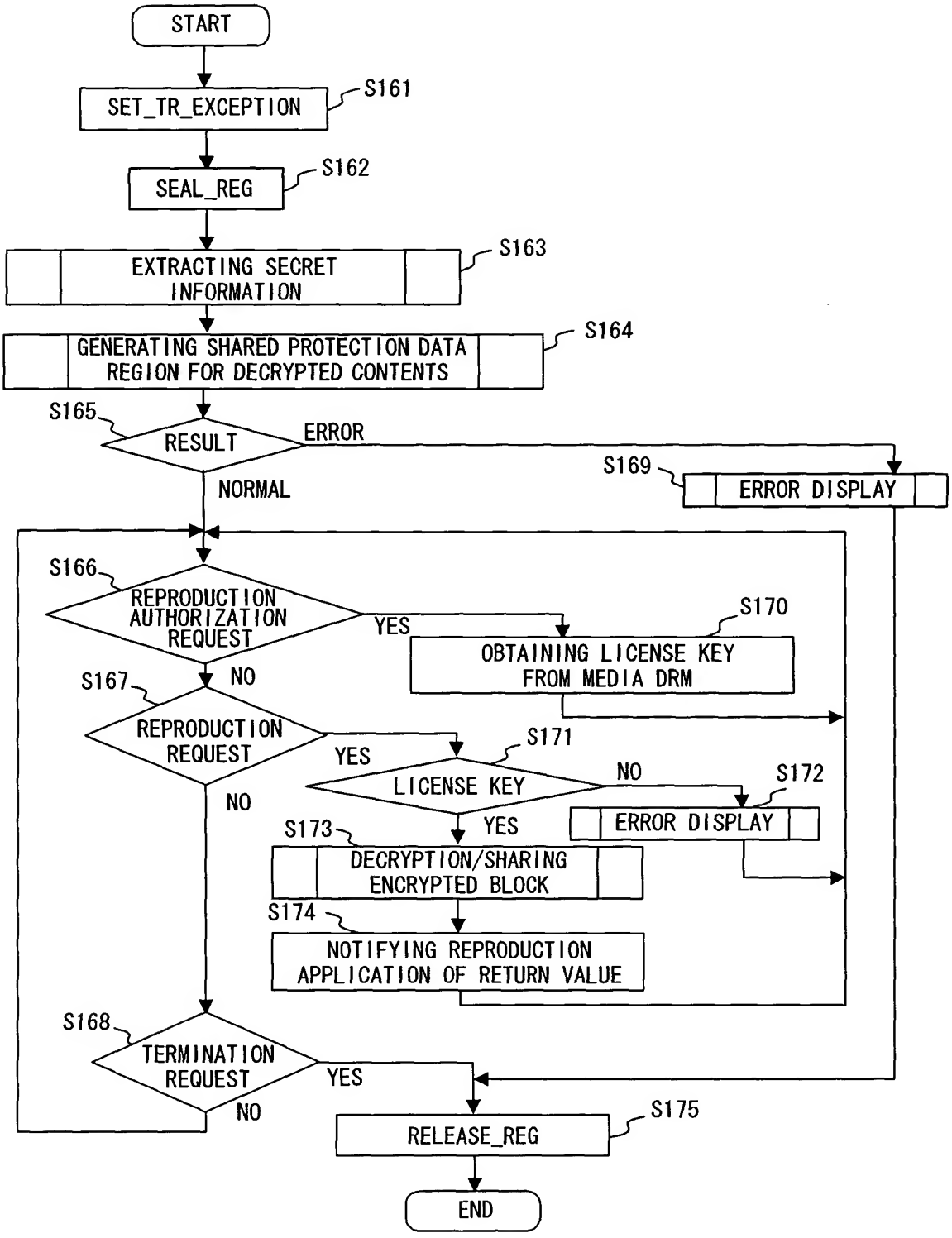

START
SET_TR_EXCEPTION
S161
SEAL_REG
S162
EXTRACTING SECRET INFORMATION
S163
GENERATING SHARED PROTECTION DATA REGION FOR DECRYPTED CONTENTS
S164
S165
RESULT
ERROR
NORMAL
S169
ERROR DISPLAY
S166
REPRODUCTION AUTHORIZATION REQUEST
YES
S170
OBTAINING LICENSE KEY FROM MEDIA DRM
NO
S167
REPRODUCTION REQUEST
YES
S171
LICENSE KEY
NO
S172
ERROR DISPLAY
NO
S173
YES
DECRYPTION/SHARING ENCRYPTED BLOCK
S174
NOTIFYING REPRODUCTION APPLICATION OF RETURN VALUE
S168
TERMINATION REQUEST
YES
NO
S175
RELEASE_REG
END

FIG. 37

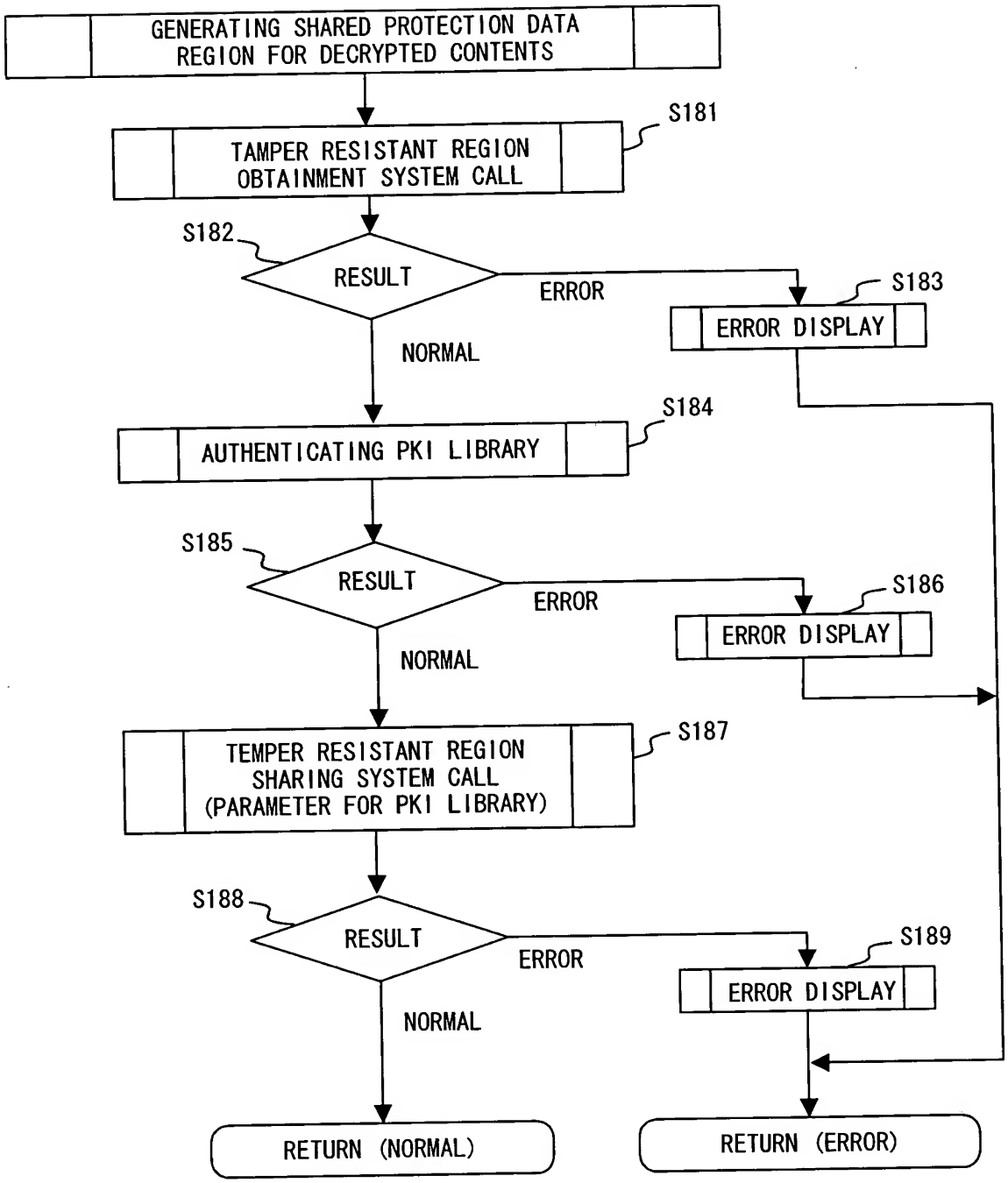

GENERATING SHARED PROTECTION DATA REGION FOR DECRYPTED CONTENTS
TAMPER RESISTANT REGION OBTAINMENT SYSTEM CALL
S181
S182
RESULT
ERROR
S183
ERROR DISPLAY
NORMAL
AUTHENTICATING PKI LIBRARY
S184
S185
RESULT
ERROR
S186
ERROR DISPLAY
NORMAL
TEMPER RESISTANT REGION SHARING SYSTEM CALL (PARAMETER FOR PKI LIBRARY)
S187
S188
RESULT
ERROR
S189
ERROR DISPLAY
NORMAL
RETURN (NORMAL)
RETURN (ERROR)

FIG. 38

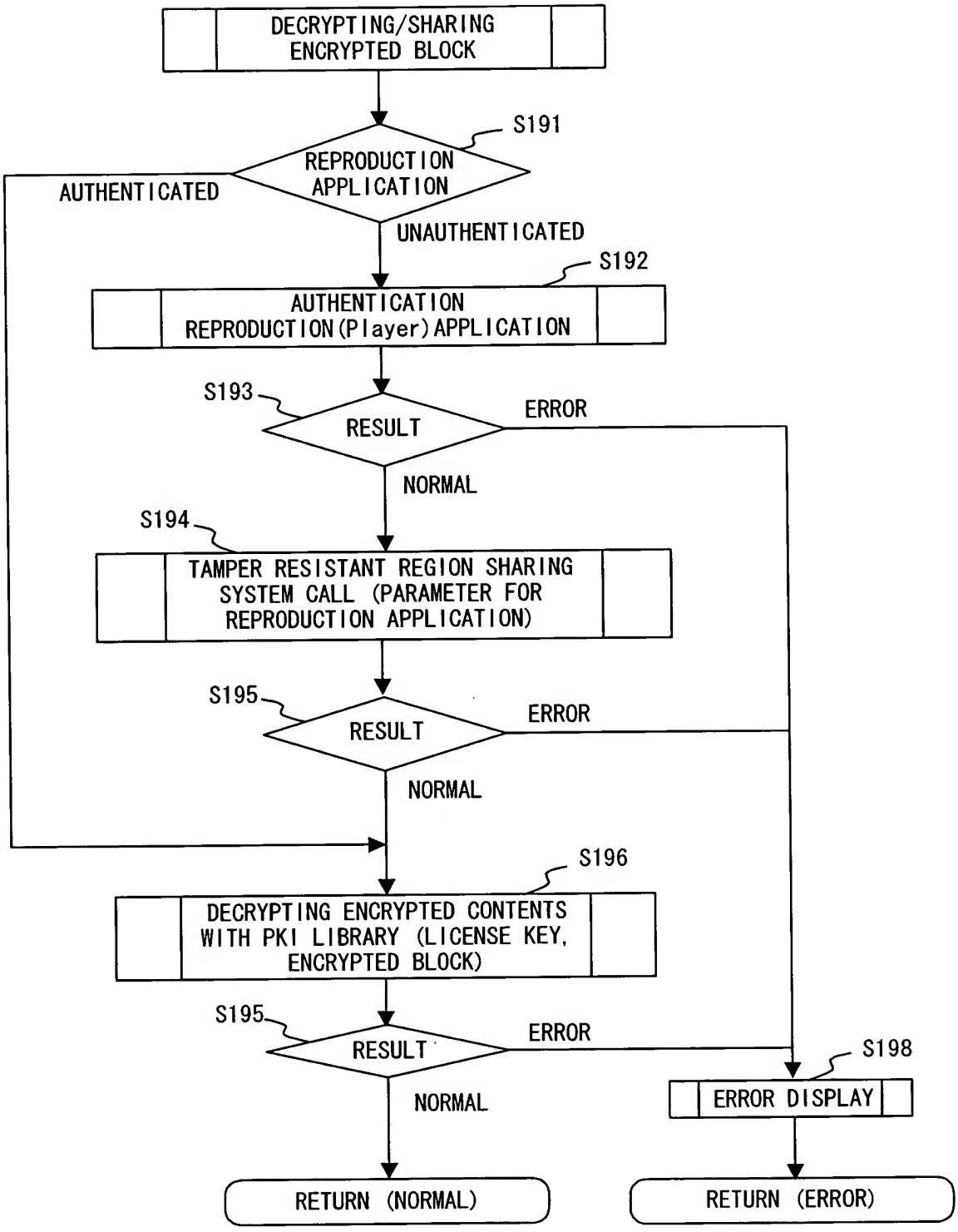

DECRYPTING/SHARING ENCRYPTED BLOCK
S191
REPRODUCTION APPLICATION
AUTHENTICATED
UNAUTHENTICATED
S192
AUTHENTICATION REPRODUCTION(Player)APPLICATION
S193
RESULT
ERROR
NORMAL
S194
TAMPER RESISTANT REGION SHARING SYSTEM CALL (PARAMETER FOR REPRODUCTION APPLICATION)
S195
RESULT
ERROR
NORMAL
S196
DECRYPTING ENCRYPTED CONTENTS WITH PKI LIBRARY (LICENSE KEY, ENCRYPTED BLOCK)
S195
RESULT
ERROR
S198
NORMAL
ERROR DISPLAY
RETURN (NORMAL)
RETURN (ERROR)

FIG. 39

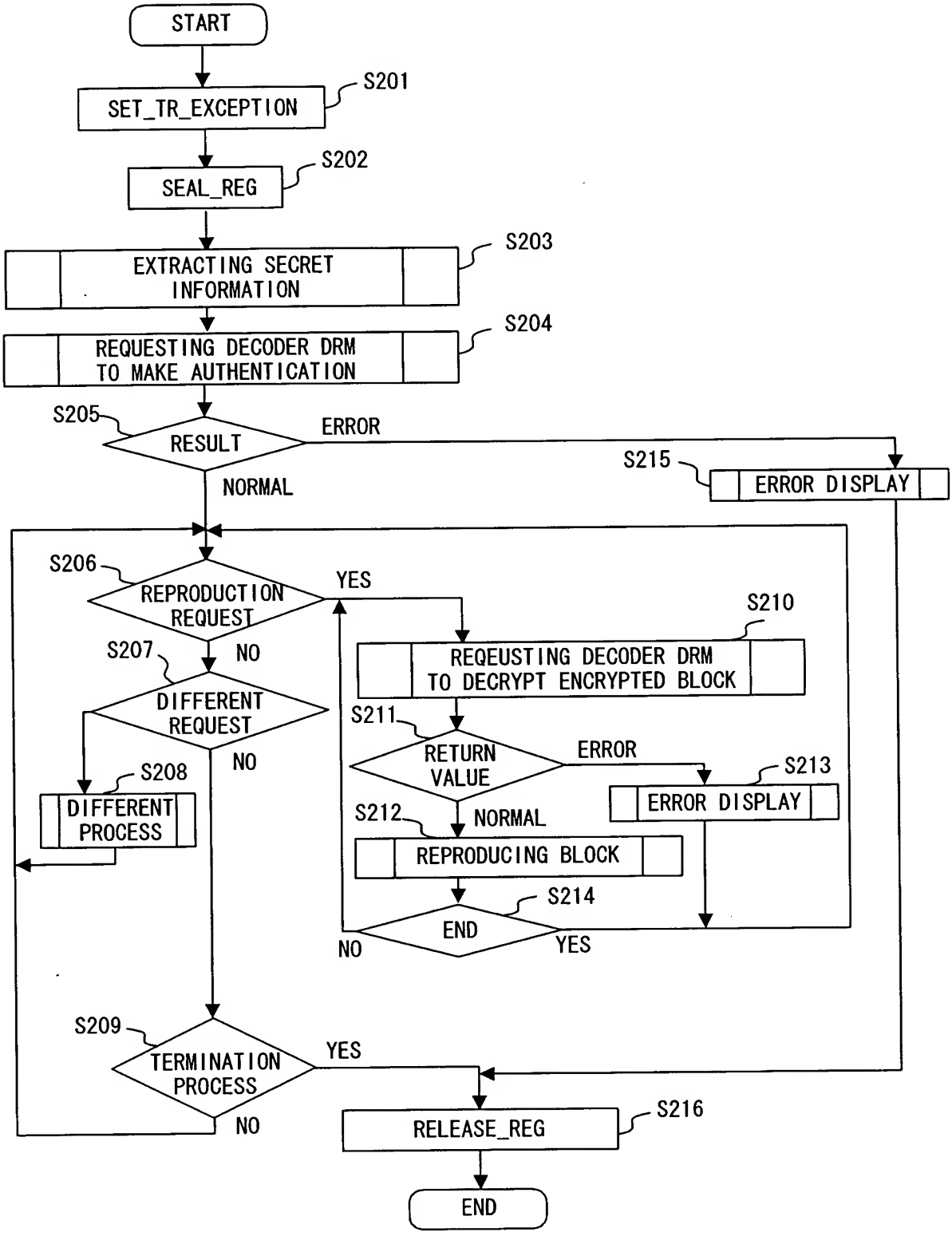

START
SET_TR_EXCEPTION
S201
SEAL_REG
S202
EXTRACTING SECRET INFORMATION
S203
REQUESTING DECODER DRM TO MAKE AUTHENTICATION
S204
S205
RESULT
ERROR
NORMAL
S215
ERROR DISPLAY
S206
REPRODUCTION REQUEST
YES
S210
REQEUSTING DECODER DRM TO DECRYPT ENCRYPTED BLOCK
S207
NO
DIFFERENT REQUEST
NO
S211
RETURN VALUE
ERROR
S213
ERROR DISPLAY
S208
DIFFERENT PROCESS
S212
NORMAL
REPRODUCING BLOCK
S214
END
NO
YES
S209
TERMINATION PROCESS
YES
NO
RELEASE_REG
S216
END

FIG. 40

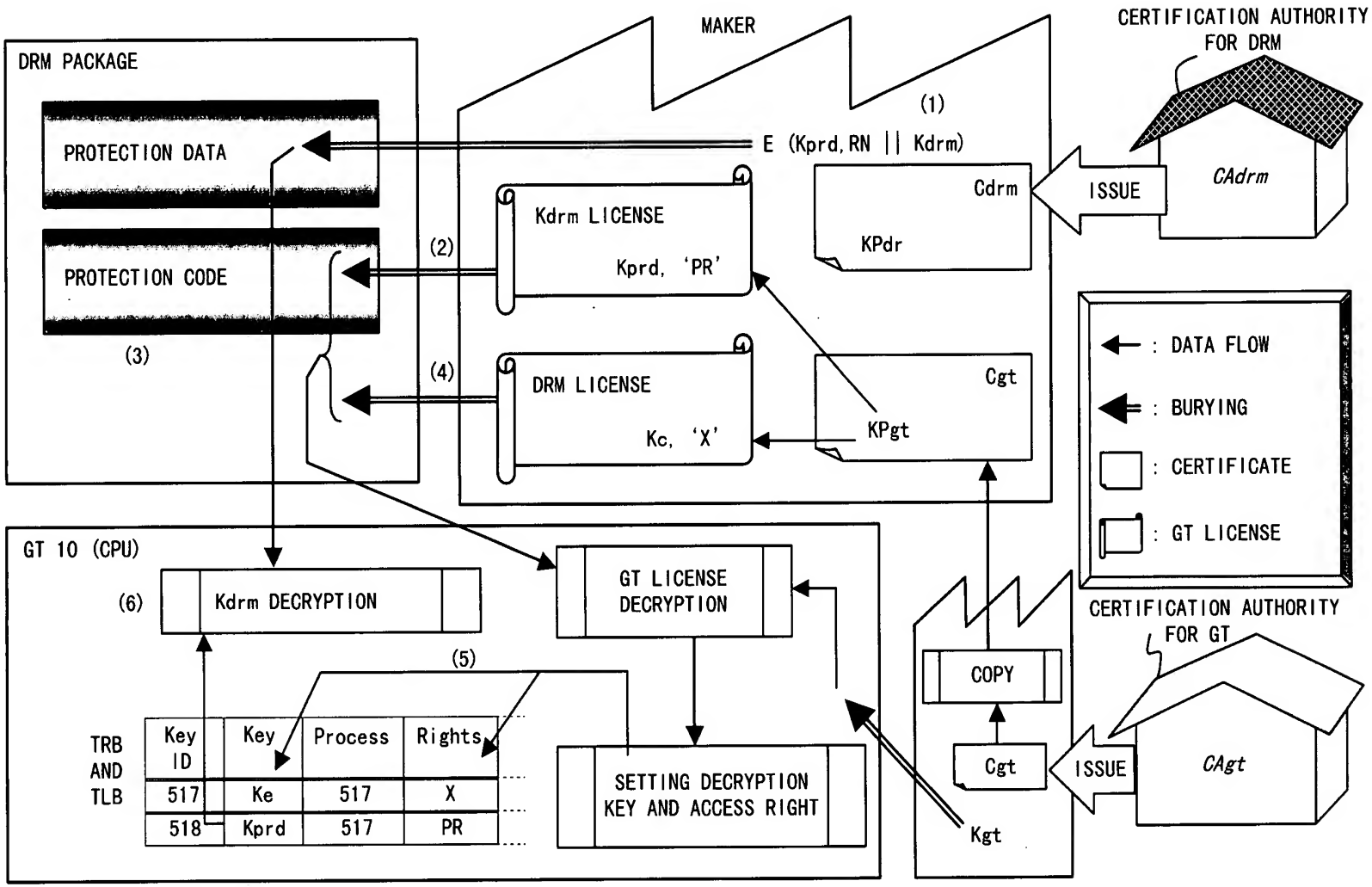

MAKER
CERTIFICATION AUTHORITY FOR DRM
DRM PACKAGE
PROTECTION DATA
PROTECTION CODE
(1)
E (Kprd, RN || Kdrm)
(2)
Kdrm LICENSE
Kprd, 'PR'
Cdrm
KPdr
ISSUE
CAdrm
(3)
(4)
DRM LICENSE
Kc, 'X'
Cgt
KPgt
: DATA FLOW
: BURYING
: CERTIFICATE
: GT LICENSE
GT 10 (CPU)
(6)
Kdrm DECRYPTION
GT LICENSE DECRYPTION
(5)
TRB AND TLB
Key ID
Key
Process
Rights
517
Ke
517
X
518
Kprd
517
PR
SETTING DECRYPTION KEY AND ACCESS RIGHT
COPY
Cgt
ISSUE
CAgt
CERTIFICATION AUTHORITY FOR GT
Kgt

FIG. 41

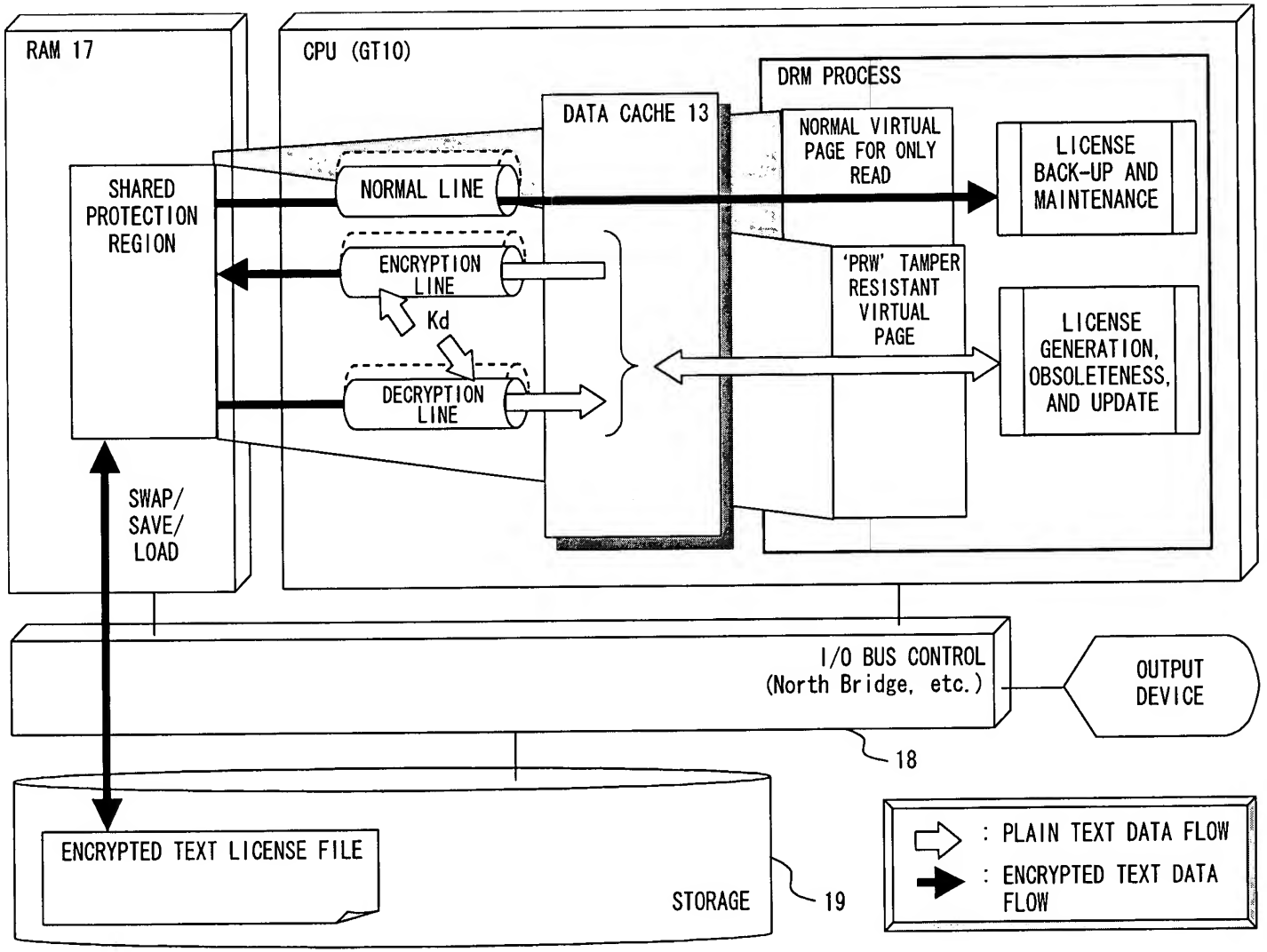

RAM 17
CPU (GT10)
DRM PROCESS
DATA CACHE 13
NORMAL VIRTUAL PAGE FOR ONLY READ
LICENSE BACK-UP AND MAINTENANCE
SHARED PROTECTION REGION
NORMAL LINE
ENCRYPTION LINE
Kd
DECRYPTION LINE
'PRW' TAMPER RESISTANT VIRTUAL PAGE
LICENSE GENERATION, OBSOLETENESS, AND UPDATE
SWAP/ SAVE/ LOAD
I/O BUS CONTROL (North Bridge, etc.)
OUTPUT DEVICE
18
ENCRYPTED TEXT LICENSE FILE
STORAGE
19
: PLAIN TEXT DATA FLOW
: ENCRYPTED TEXT DATA FLOW

FIG. 42

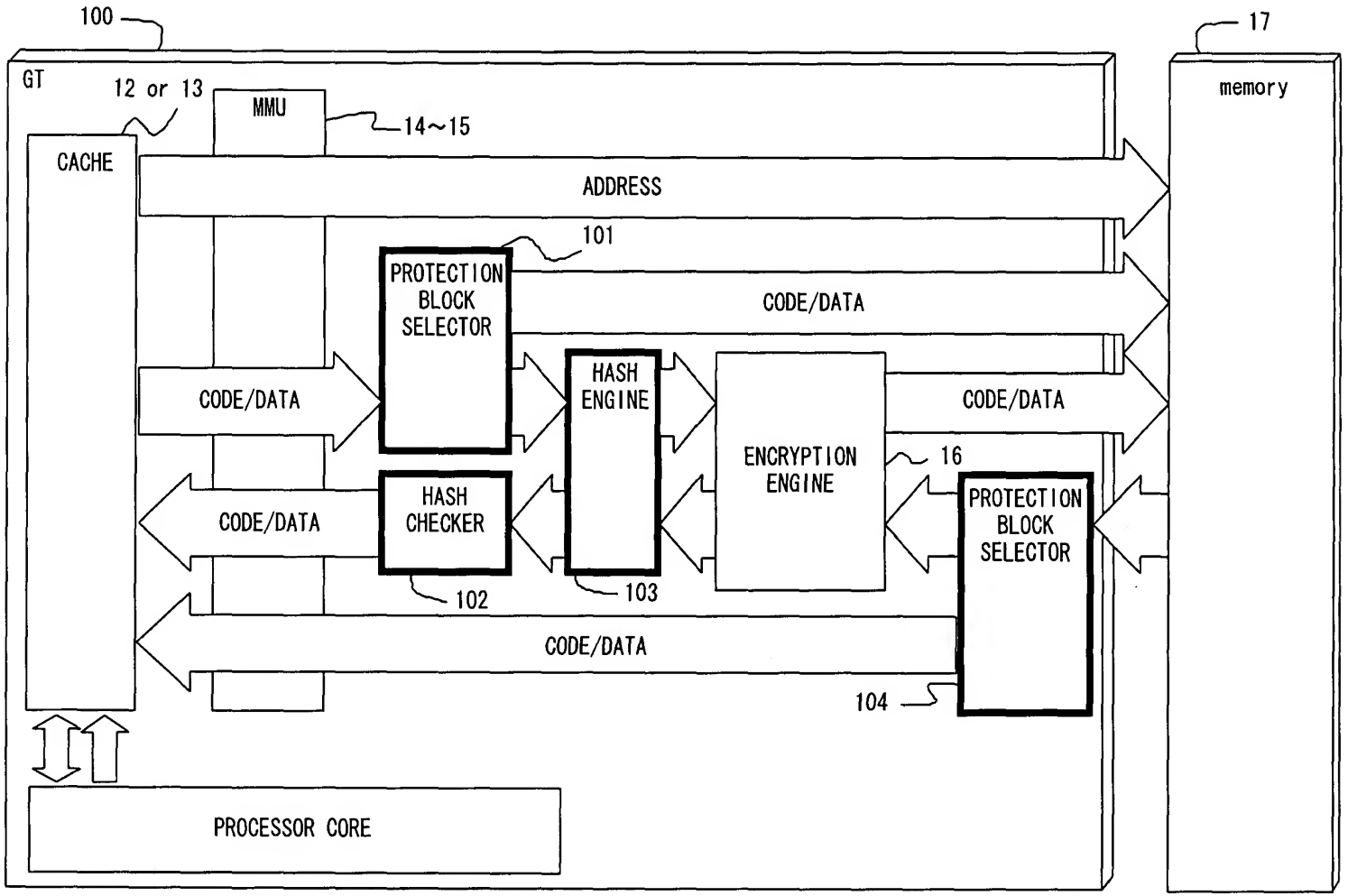

100
17
GT
12 or 13
MMU
14~15
memory
CACHE
ADDRESS
101
PROTECTION BLOCK SELECTOR
CODE/DATA
HASH ENGINE
CODE/DATA
CODE/DATA
ENCRYPTION ENGINE
16
HASH CHECKER
CODE/DATA
PROTECTION BLOCK SELECTOR
102
103
CODE/DATA
104
PROCESSOR CORE

FIG. 43

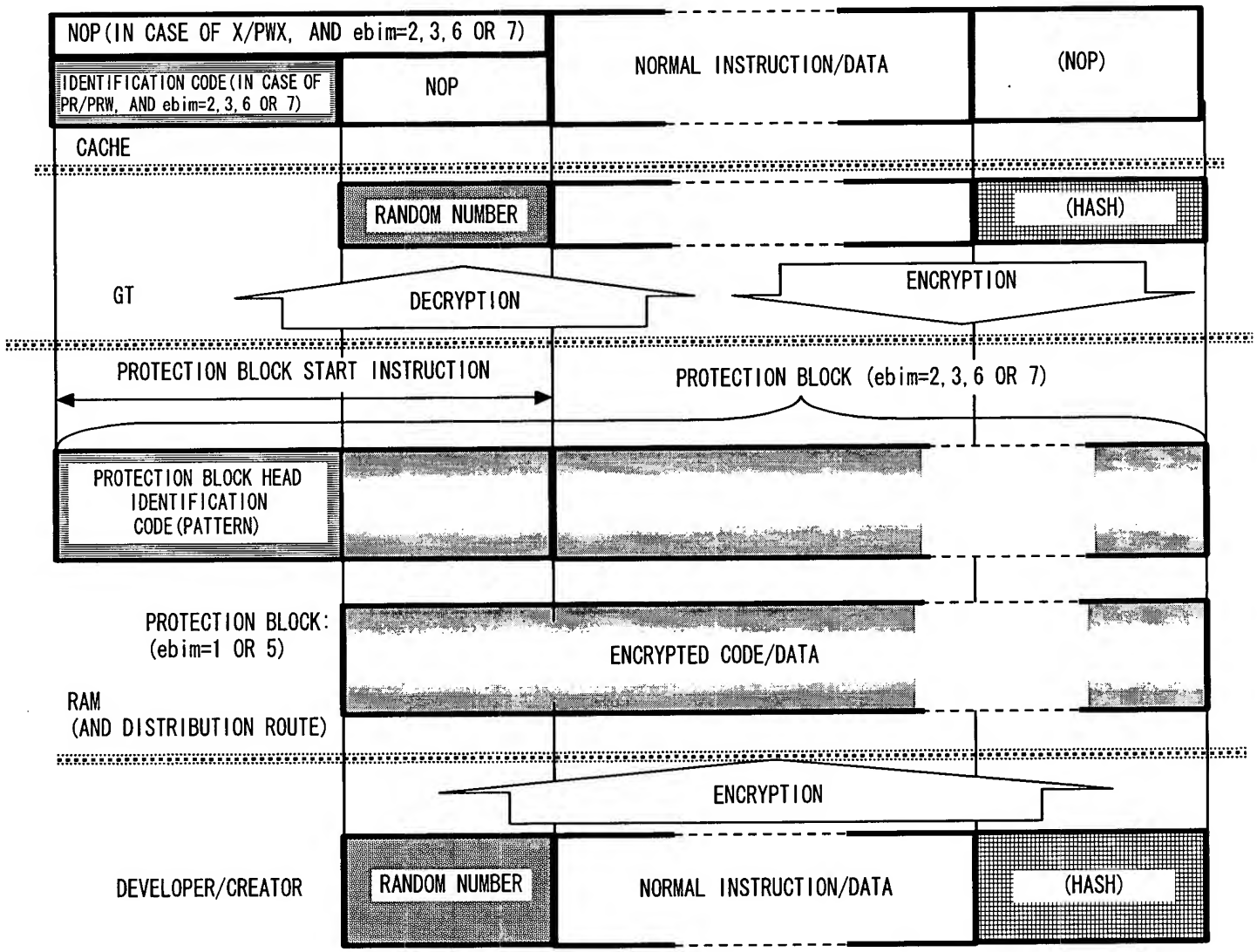

NOP(IN CASE OF X/PWX, AND ebim=2,3,6 OR 7)
IDENTIFICATION CODE(IN CASE OF PR/PRW, AND ebim=2,3,6 OR 7)
NOP
NORMAL INSTRUCTION/DATA
(NOP)
CACHE
RANDOM NUMBER
(HASH)
GT
DECRYPTION
ENCRYPTION
PROTECTION BLOCK START INSTRUCTION
PROTECTION BLOCK (ebim=2,3,6 OR 7)
PROTECTION BLOCK HEAD IDENTIFICATION CODE(PATTERN)
PROTECTION BLOCK: (ebim=1 OR 5)
ENCRYPTED CODE/DATA
RAM (AND DISTRIBUTION ROUTE)
ENCRYPTION
DEVELOPER/CREATOR
RANDOM NUMBER
NORMAL INSTRUCTION/DATA
(HASH)

FIG. 44

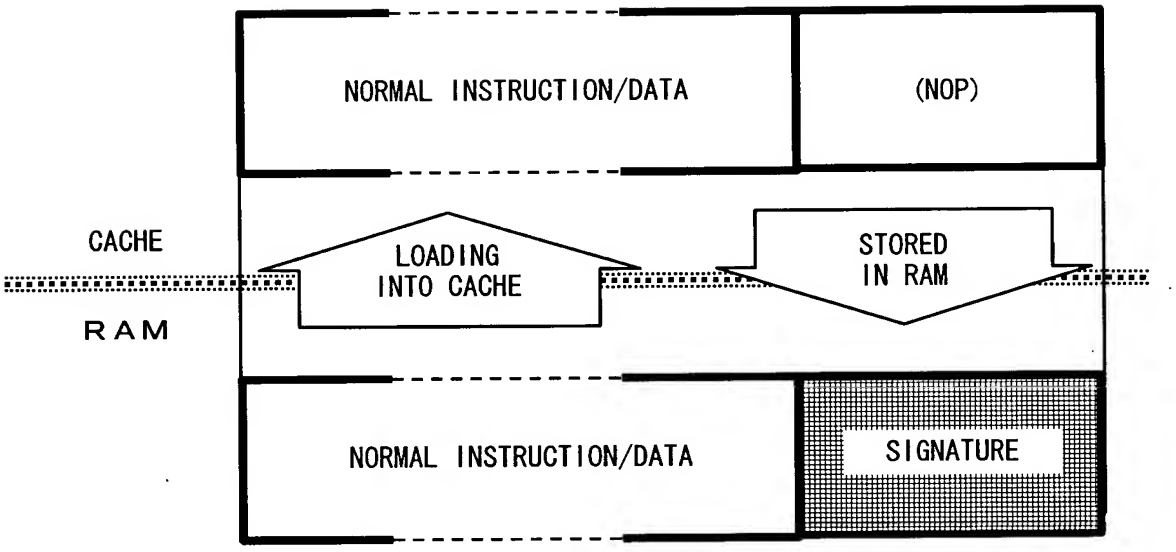

NORMAL INSTRUCTION/DATA
(NOP)
CACHE
LOADING
INTO CACHE
STORED
IN RAM
RAM
NORMAL INSTRUCTION/DATA
SIGNATURE

FIG. 45

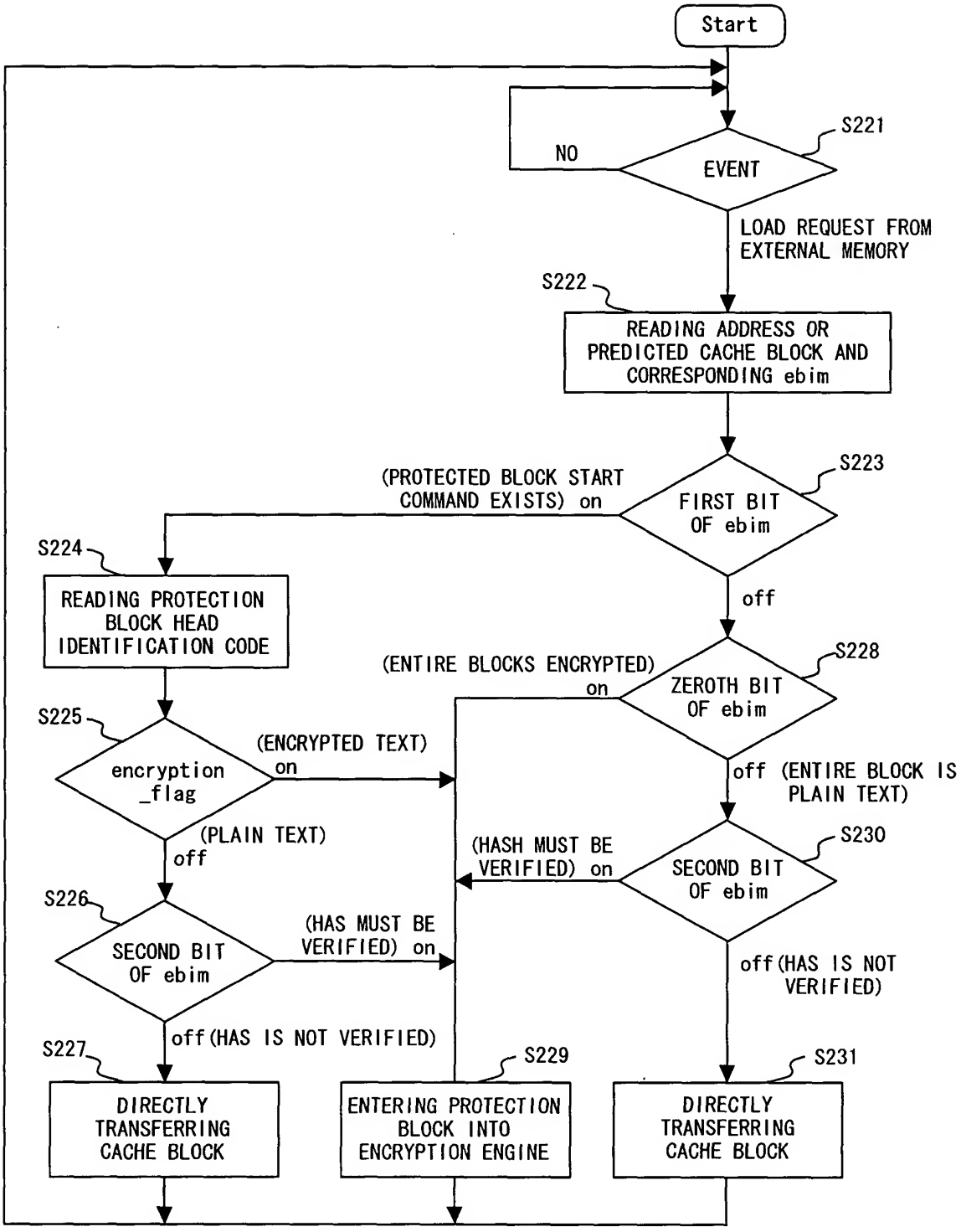
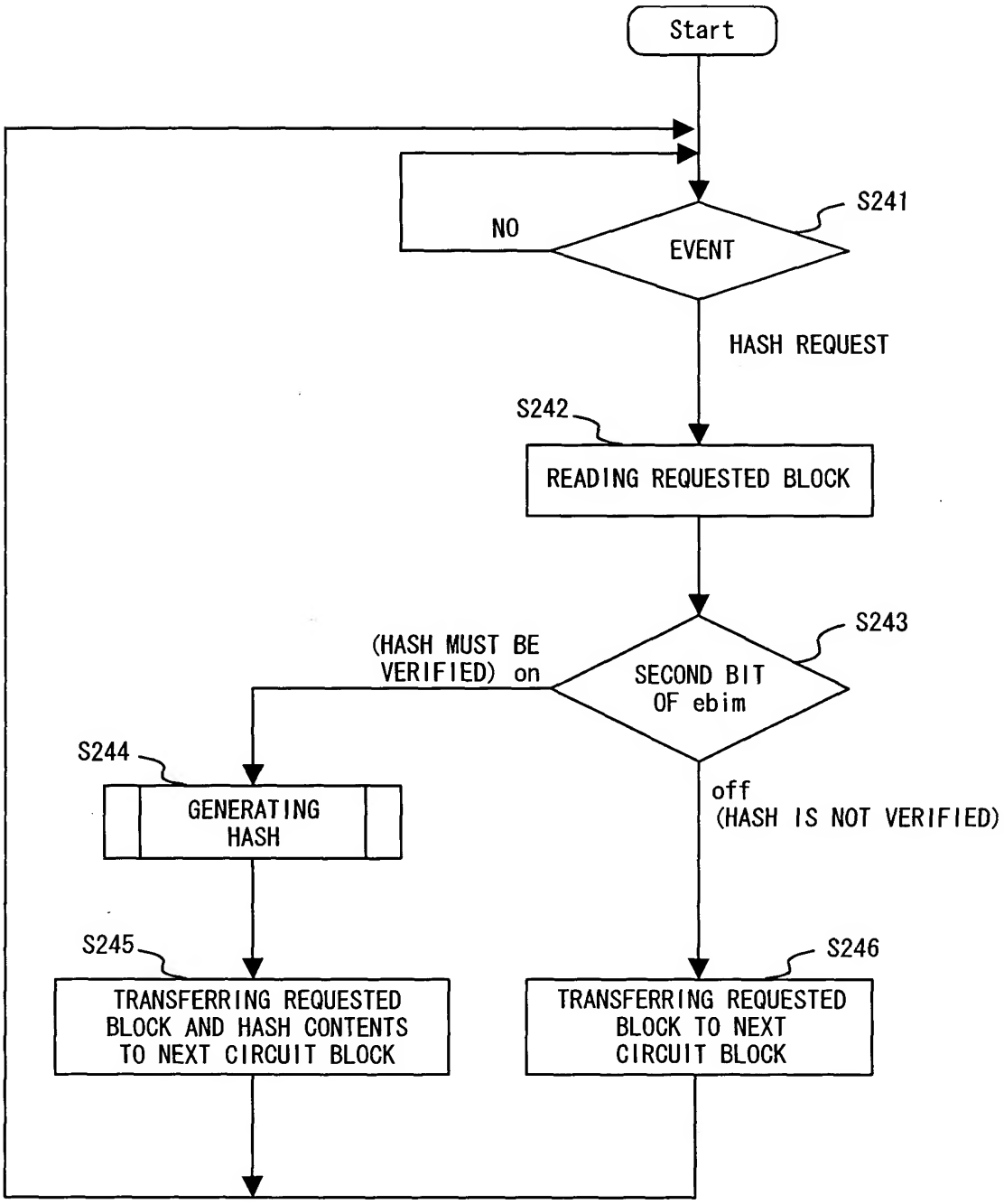

Start
S221
NO
EVENT
LOAD REQUEST FROM EXTERNAL MEMORY
S222
READING ADDRESS OR PREDICTED CACHE BLOCK AND CORRESPONDING ebim
S223
(PROTECTED BLOCK START COMMAND EXISTS) on
FIRST BIT OF ebim
off
S224
READING PROTECTION BLOCK HEAD IDENTIFICATION CODE
S228
(ENTIRE BLOCKS ENCRYPTED) on
ZEROTH BIT OF ebim
S225
encryption _flag
(ENCRYPTED TEXT) on
off (ENTIRE BLOCK IS PLAIN TEXT)
(PLAIN TEXT) off
S230
(HASH MUST BE VERIFIED) on
SECOND BIT OF ebim
S226
SECOND BIT OF ebim
(HAS MUST BE VERIFIED) on
off(HAS IS NOT VERIFIED)
off(HAS IS NOT VERIFIED)
S227
S229
S231
DIRECTLY TRANSFERRING CACHE BLOCK
ENTERING PROTECTION BLOCK INTO ENCRYPTION ENGINE
DIRECTLY TRANSFERRING CACHE BLOCK

FIG. 46


Start
S241
NO
EVENT
HASH REQUEST
S242
READING REQUESTED BLOCK
S243
(HASH MUST BE VERIFIED) on
SECOND BIT OF ebim
S244
GENERATING HASH
off
(HASH IS NOT VERIFIED)
S245
TRANSFERRING REQUESTED BLOCK AND HASH CONTENTS TO NEXT CIRCUIT BLOCK
S246
TRANSFERRING REQUESTED BLOCK TO NEXT CIRCUIT BLOCK

F I G. 4 7

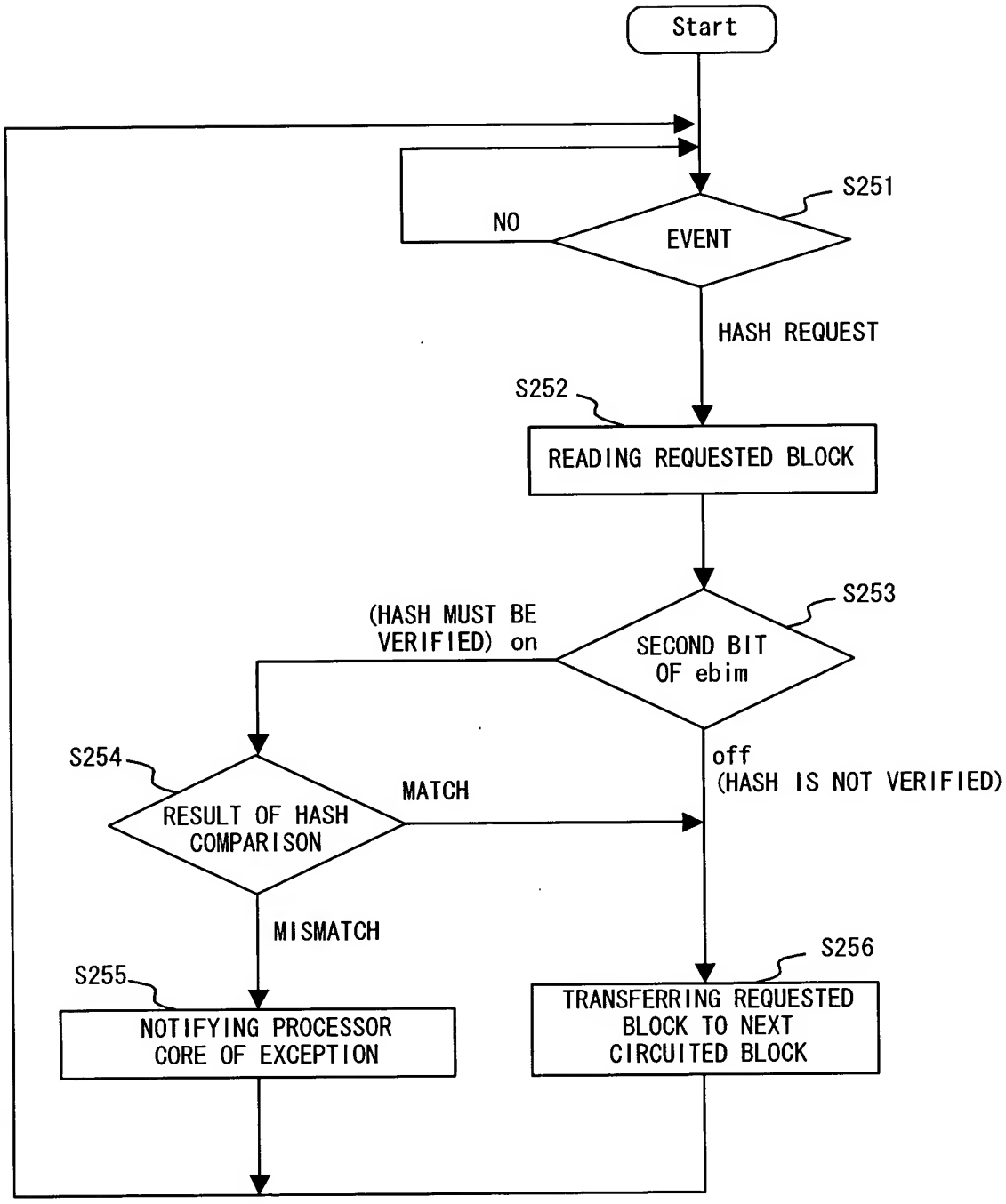

Start
S251
NO
EVENT
HASH REQUEST
S252
READING REQUESTED BLOCK
S253
(HASH MUST BE VERIFIED) on
SECOND BIT OF ebim
off
(HASH IS NOT VERIFIED)
S254
RESULT OF HASH COMPARISON
MATCH
MISMATCH
S255
NOTIFYING PROCESSOR CORE OF EXCEPTION
S256
TRANSFERRING REQUESTED BLOCK TO NEXT CIRCUITED BLOCK

FIG. 48

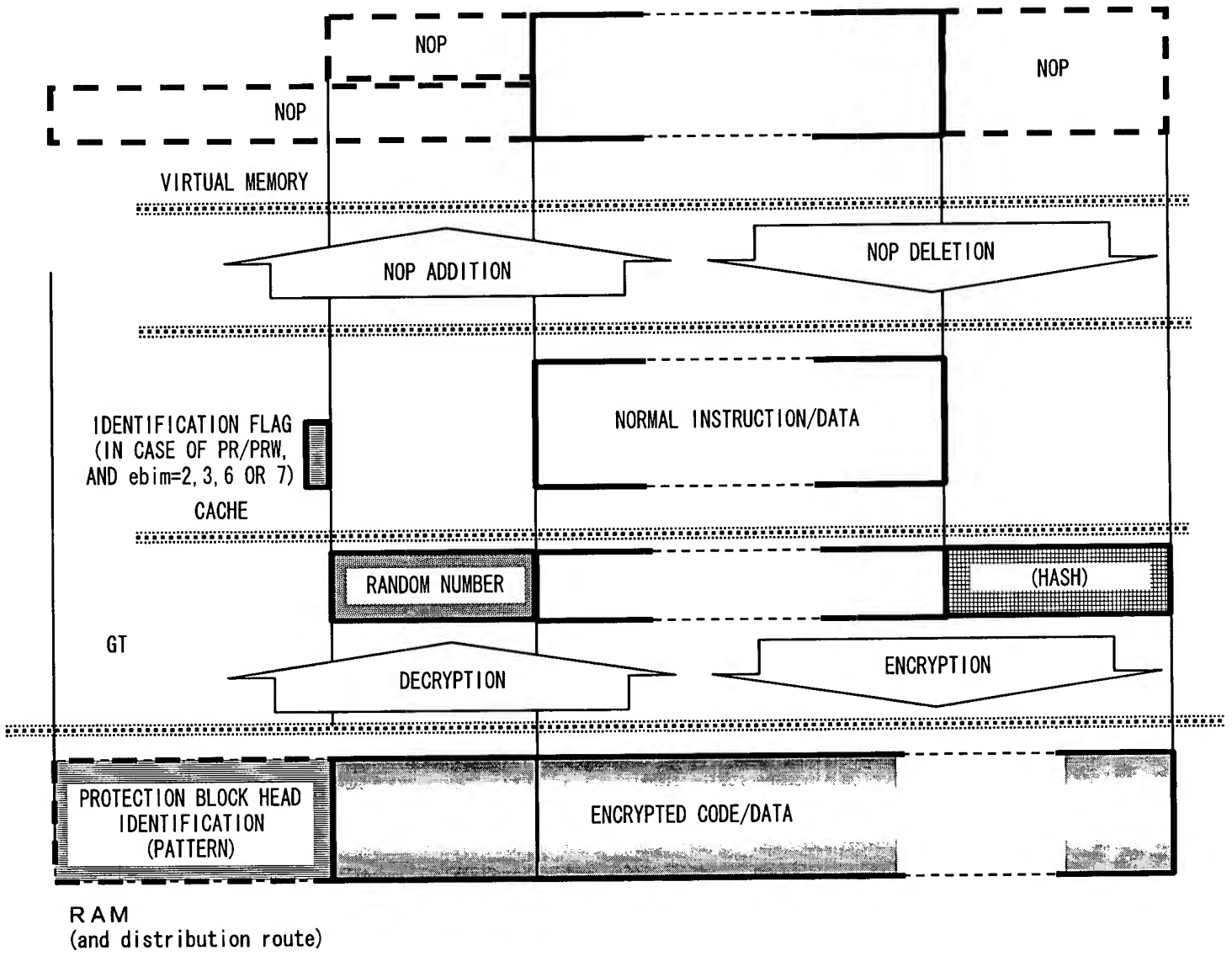

NOP
NOP
NOP
VIRTUAL MEMORY
NOP ADDITION
NOP DELETION
IDENTIFICATION FLAG
(IN CASE OF PR/PRW,
AND ebim=2, 3, 6 OR 7)
NORMAL INSTRUCTION/DATA
CACHE
RANDOM NUMBER
(HASH)
GT
DECRYPTION
ENCRYPTION
PROTECTION BLOCK HEAD
IDENTIFICATION
(PATTERN)
ENCRYPTED CODE/DATA
RAM
(and distribution route)

FIG. 49

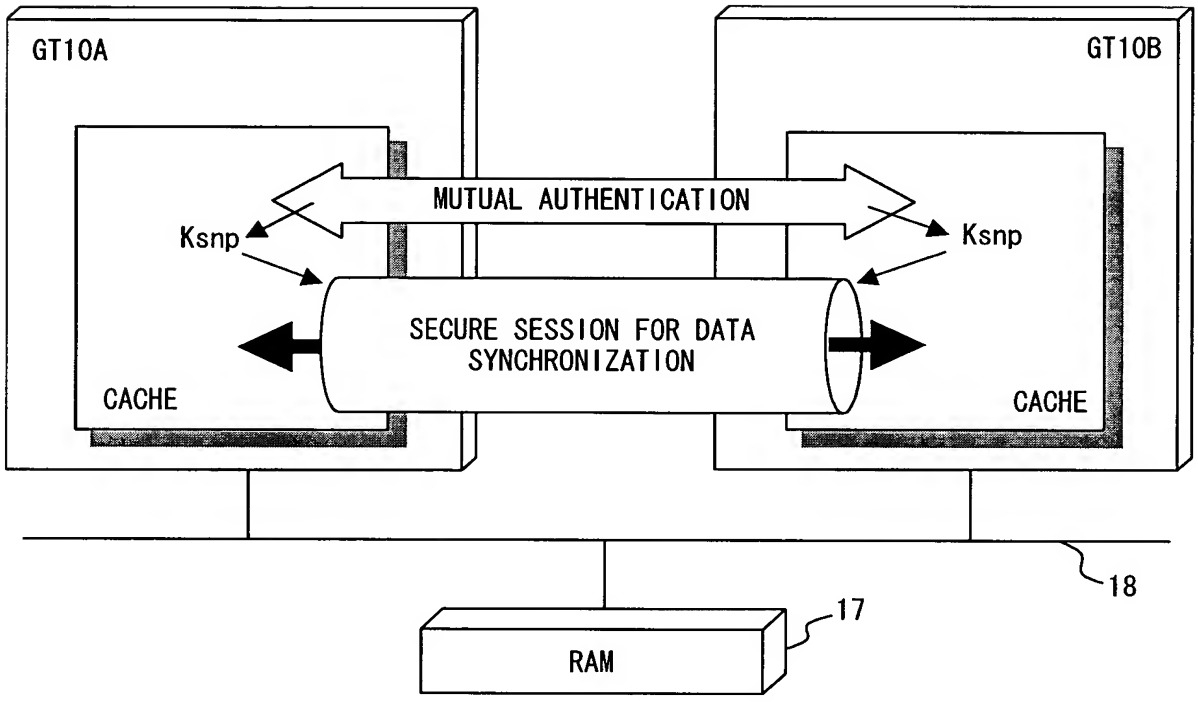

GT10A
GT10B
MUTUAL AUTHENTICATION
Ksnp
Ksnp
SECURE SESSION FOR DATA SYNCHRONIZATION
CACHE
CACHE
18
17
RAM

FIG. 50

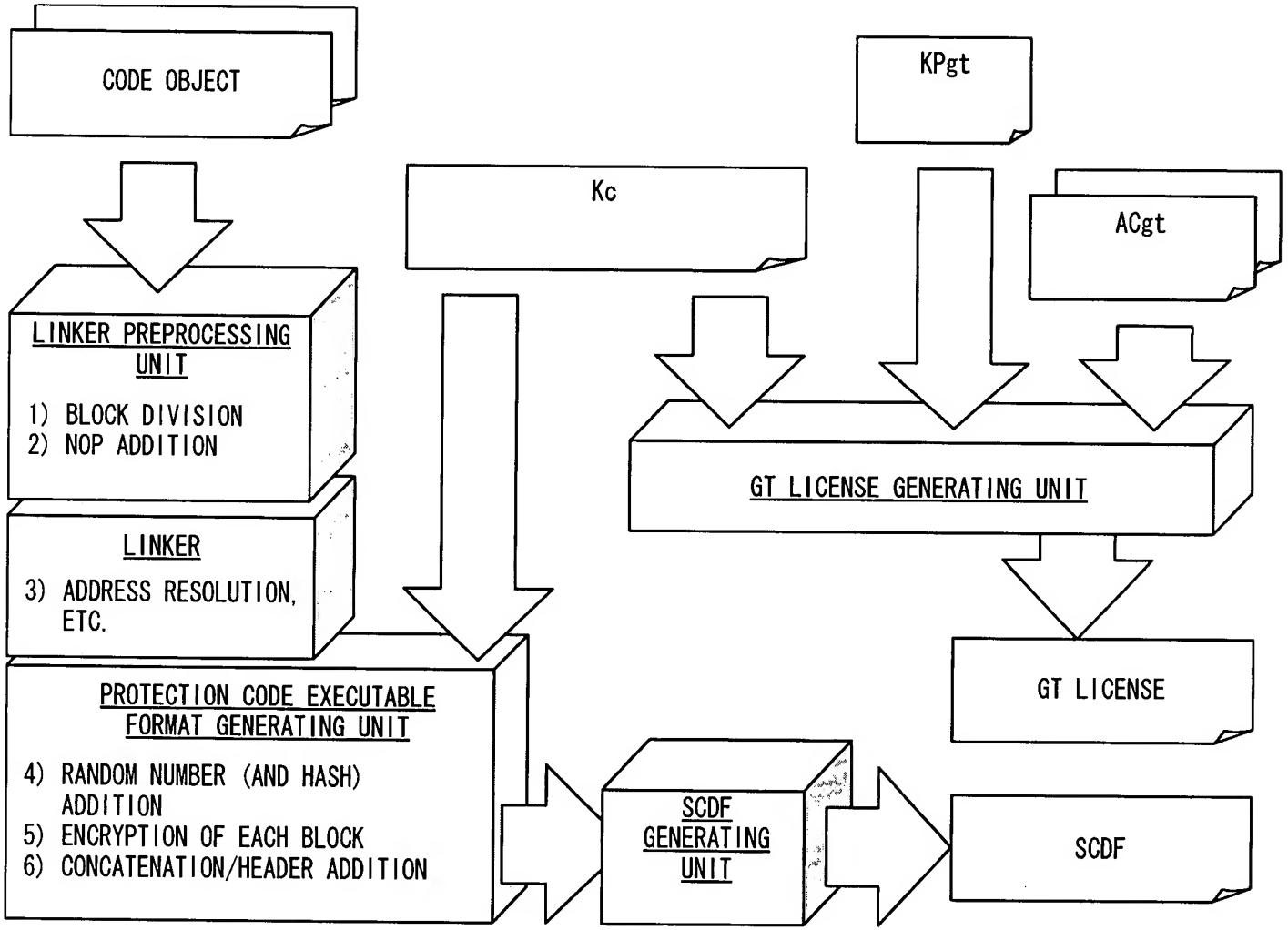

CODE OBJECT
KPgt
Kc
ACgt
LINKER PREPROCESSING UNIT
1) BLOCK DIVISION
2) NOP ADDITION
GT LICENSE GENERATING UNIT
LINKER
3) ADDRESS RESOLUTION, ETC.
GT LICENSE
PROTECTION CODE EXECUTABLE FORMAT GENERATING UNIT
4) RANDOM NUMBER (AND HASH) ADDITION
5) ENCRYPTION OF EACH BLOCK
6) CONCATENATION/HEADER ADDITION
SCDF GENERATING UNIT
SCDF

FIG. 51

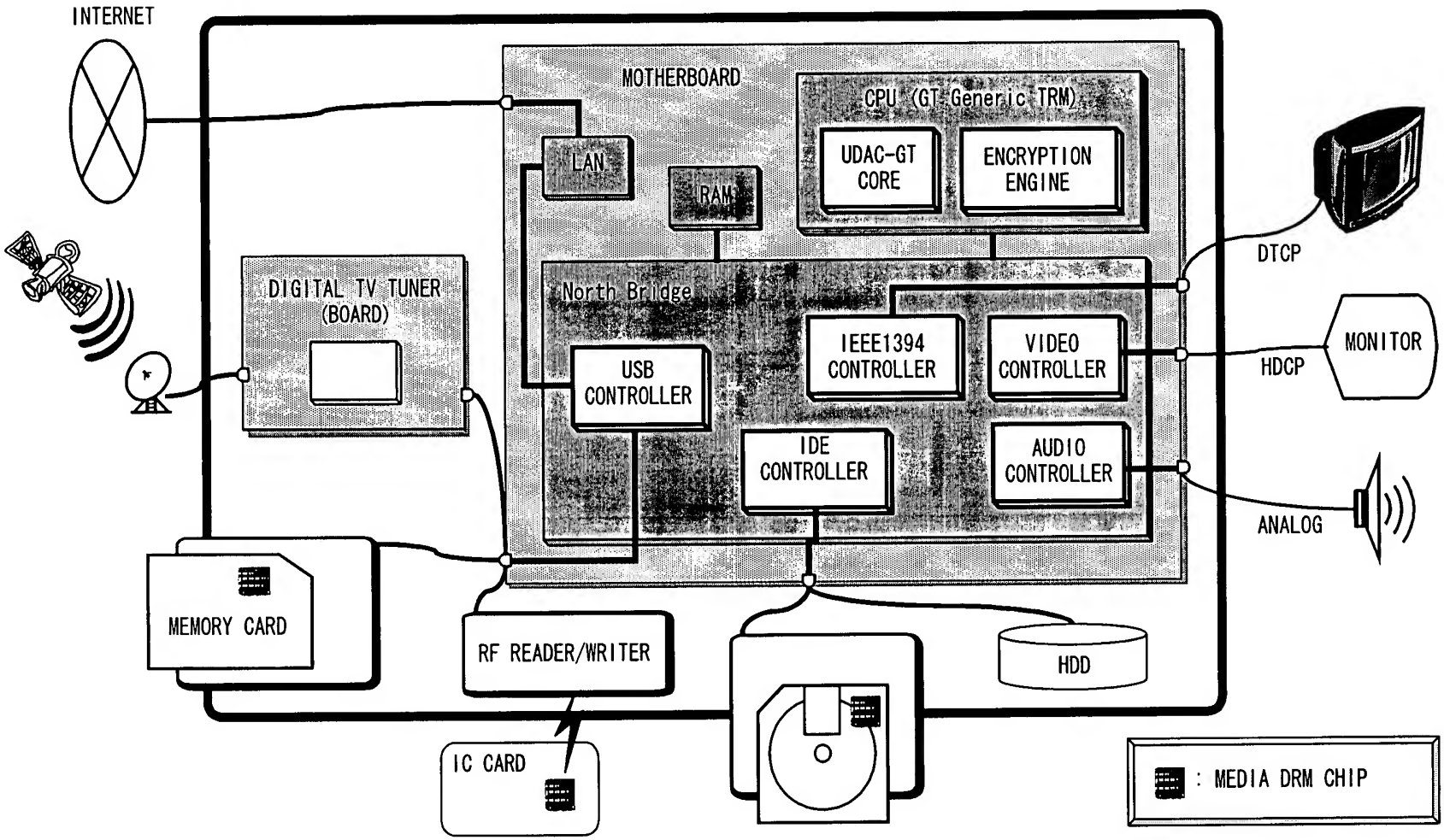

INTERNET
MOTHERBOARD
CPU (GT Generic TRM)
UDAC-GT CORE
ENCRYPTION ENGINE
LAN
RAM
North Bridge
USB CONTROLLER
IEEE1394 CONTROLLER
VIDEO CONTROLLER
IDE CONTROLLER
AUDIO CONTROLLER
DIGITAL TV TUNER (BOARD)
DTCP
HDCP
MONITOR
ANALOG
MEMORY CARD
RF READER/WRITER
HDD
IC CARD
: MEDIA DRM CHIP

FIG. 52